Identificación y Gestión de Riesgos

Durante el proceso de desarrollo y funcionamiento del proyecto, existen diversos riesgos que podrían surgir. A continuación, se enumeran algunos de los posibles riesgos a tener en cuenta:

Caída de los servidores: Existe la posibilidad de que los servidores experimenten interrupciones o fallos técnicos, lo cual podría afectar el acceso y la disponibilidad del proyecto.

Cambios en los requerimientos del cliente: Es posible que el cliente solicite modificaciones o cambios en los requisitos iniciales del proyecto, lo cual podría impactar en los plazos, costos y alcance acordados.

Hackeo a nivel de base de datos: Existe el riesgo de que la base de datos sea objeto de ataques cibernéticos, lo cual podría comprometer la seguridad y la integridad de los datos almacenados.

Problemas en el respaldo de los datos: Si no se realizan copias de seguridad periódicas y efectivas de la base de datos, se corre el riesgo de perder información importante en caso de fallos o incidentes.

Corrupción del programa: Puede ocurrir que el programa o software utilizado para el proyecto se corrompa, lo cual podría provocar errores o mal funcionamiento en la aplicación.

Mal manejo a nivel de mantenimiento: Si no se lleva a cabo un adecuado mantenimiento del proyecto, podrían surgir problemas de rendimiento, seguridad y estabilidad a lo largo del tiempo.

Además de los riesgos mencionados, es importante tener en cuenta las siguientes excepciones y eventos externos que podrían afectar el proyecto:

Solicitud de entrega anticipada: Si el cliente requiere que el proyecto se entregue antes de la fecha acordada inicialmente, se aplicará una multa adicional para cubrir los costos y esfuerzos adicionales necesarios.

Incendios o inundaciones: Eventos naturales como incendios o inundaciones podrían dañar el equipo, los servidores o las instalaciones físicas, lo cual podría causar retrasos en el desarrollo o interrupciones en el funcionamiento.

Corte de luz: Interrupciones en el suministro eléctrico pueden ocasionar la inoperatividad temporal del proyecto y afectar los plazos establecidos.

Es fundamental evaluar y mitigar estos riesgos, así como establecer medidas de seguridad y protocolos de contingencia para minimizar su impacto en el proyecto y garantizar su éxito.

Es importante destacar que esta lista de riesgos y excepciones no es exhaustiva, y se recomienda llevar a cabo un análisis de riesgos más detallado y adaptado a las circunstancias específicas del proyecto.

Plan de Contingencia:

El objetivo del plan de contingencia es identificar y abordar los posibles riesgos y eventos adversos que podrían surgir durante el desarrollo y funcionamiento del proyecto. A continuación, se presenta un plan de contingencia basado en los riesgos mencionados anteriormente:

Caída de los servidores:

Establecer un acuerdo de nivel de servicio (SLA) con el proveedor de servicios de hosting para garantizar un tiempo de actividad mínimo y un soporte rápido en caso de interrupciones, si llega a suceder algo el mantenimiento vendría en 12 horas o como mucho 24 horas.

Mantener un monitoreo constante de los servidores para detectar cualquier problema o anomalía en el rendimiento.

Implementar un plan de respaldo y recuperación que permita restaurar rápidamente los servicios en caso de caída de los servidores.

Cambios en los requerimientos del cliente:

Establecer una comunicación clara y regular con el cliente para comprender y documentar los requisitos iniciales de manera precisa.

Implementar un proceso de gestión de cambios formal, donde cualquier modificación solicitada por el cliente se evalúe en términos de impacto en los plazos, costos y alcance del proyecto.

Mantener una documentación actualizada de los cambios acordados y obtener la aprobación del cliente antes de implementarlos.

Hackeo a nivel de base de datos:

Aplicar medidas de seguridad sólidas, como el cifrado de datos, autenticación de usuarios y protección contra ataques conocidos.

Realizar auditorías de seguridad regulares para identificar y corregir posibles vulnerabilidades.

Establecer políticas de seguridad de acceso y realizar copias de seguridad periódicas de la base de datos.

Problemas en el respaldo de los datos:

Establecer una programación automática y regular de copias de seguridad de la base de datos.

Verificar periódicamente la integridad de las copias de seguridad y realizar pruebas de restauración para garantizar que los datos se puedan recuperar correctamente.

Corrupción del programa:

Implementar un sistema de control de versiones para rastrear y revertir cambios en el código en caso de corrupción o errores.

Realizar pruebas exhaustivas y pruebas de calidad para identificar y corregir posibles problemas antes de implementar nuevas versiones.

Mal manejo a nivel de mantenimiento:

Establecer un plan de mantenimiento regular que incluya actualizaciones de seguridad, correcciones de errores y optimizaciones de rendimiento.

Asignar recursos y personal dedicado para realizar el mantenimiento adecuado y seguimiento de los indicadores clave de rendimiento.

Excepciones y eventos externos:

Solicitud de entrega anticipada:

Establecer cláusulas contractuales que especifiquen las implicaciones financieras y logísticas de una entrega anticipada.

Evaluar los recursos disponibles y los impactos potenciales en la calidad y la satisfacción del cliente antes de aceptar una entrega anticipada.

Incendios o inundaciones:

Implementar medidas de seguridad y protección adecuadas, como sistemas de extinción de incendios y almacenamiento seguro de equipos y datos.

Establecer planes de evacuación y continuidad del negocio en caso de desastres naturales.

Realizar copias de seguridad y almacenamiento externo de datos importantes para mitigar el riesgo de pérdida.

Corte de luz:

Contar con fuentes de energía alternativas, como generadores o sistemas de respaldo de energía, para garantizar la continuidad del servicio durante cortes de energía.

Establecer protocolos de respaldo y apagado seguro de los sistemas en caso de corte prolongado.

Es importante revisar y actualizar regularmente el plan de contingencia para abordar cualquier cambio en los riesgos y circunstancias del proyecto. Además, es fundamental capacitar al personal involucrado en el proyecto sobre el plan de contingencia y realizar simulacros de crisis para asegurar una respuesta efectiva en caso de que ocurra alguna contingencia.