LINKUNI - RIESGOS

RIESGO 001. Suplantación de cuenta de usuario

- **Descripción:**

Se produce un ataque informático, por lo que el atacante logra hacerse con el control de distintas cuentas. Consigue realizar una suplantación del usuario afectado y así hacerse pasar por él.

- **Probabilidad:**

Verosímil.

- **Impacto:**

El usuario afectado, si no puede recuperar su cuenta, tendrá que crear una nueva. Esto puede provocar que las víctimas dejen de utilizar nuestro sistema. Además, el atacante podría aprovecharse maliciosamente de la cuenta robada.

- **Indicadores:**

El usuario afectado lo comunica a nuestro equipo a través de una incidencia.

- **Estrategias de prevención:**

Mejorar la seguridad en el ámbito de la accesibilidad de los usuarios. Empleando, por ejemplo, contraseñas bastante difíciles de descifrar.

- **Planes de mitigación:**

Eliminar al atacante de nuestro sistema y recuperar la cuenta robada al usuario pertinente.

RIESGO 002. Rastreo no deseado

- **Descripción:**

Un usuario es rastreado geológicamente, cuando este usuario no había compartido su localización con el resto de usuarios.

- **Probabilidad:**

Poco probable.

- **Impacto:**

Un usuario localizado puede causar repercusiones por su propia seguridad.

- **Indicadores:**

El sistema comunicará el acceso no deseado a la ubicación de un usuario.

- **Estrategias de prevención:**

Utilizar servidores con restricciones de firewall muy seguras.

- **Planes de mitigación:**

Rastrear el origen del ataque y prohibir el acceso al sistema al causante.

RIESGO 003. Acceso a la base de datos

- **Descripción:**

Se produce un acceso a la base de datos de nuestro sistema causado por un ataque informático.

- **Probabilidad:**

Poco probable.

- **Impacto:**

La información de los usuarios afectados estaría disponible por el atacante y esto violaría la ley de protección de datos.

- **Indicadores:**

El sistema comunicará el acceso no deseado a la base de datos.

- **Estrategias de prevención:**

Disponer de una base de datos lo suficientemente fuerte como para prevenir ataques informáticos.

- **Planes de mitigación:**

Rastrear el origen del ataque y prohibir el acceso al sistema al causante. Además, debería mejorarse la seguridad de la base de datos.

RIESGO 004. Número de usuarios insuficientes

- **Descripción:**

El número de usuarios que utilizan nuestro sistema software es insuficiente, por lo que no podríamos sostener el proyecto.

- **Probabilidad:**

Verosímil.

- **Impacto:**

Si no fuéramos capaces de sostener el proyecto, esto impediría que la universidad mantuviese los servidores y bases de datos.

- **Indicadores:**

Cantidad de usuarios registrados en la base de datos.

- **Estrategias de prevención:**

Tener buen mantenimiento de la aplicación a lo largo de la vida del sistema. Utilizar técnicas de publicidad lo suficientemente buenas para llegar a nuestros clientes.

- **Planes de mitigación:**

Identificar y cambiar posibles causas del reducido número de usuarios, así como realizar un anuncio publicitario con el fin de intentar salvar el proyecto.

RIESGO 005. Fallos de Servidor/base datos

- **Descripción:**

Debido a factores externos o ajenos al sistema falla el servidor o la base de datos

- **Probabilidad:**

Poco probable.

- **Impacto:**

El servicio queda bloqueado hasta que se solucione el problema con el servidor/base de datos.

- **Indicadores:**

No se puede acceder al sistema/ iniciar sesión.

- **Estrategias de prevención:**

Utilizar servidores con más capacidad para soportar grandes cantidades de usuarios, tener los servidores en lugares seguros, que no se puedan producir fallos por sobrecalentamiento, incendio, inundación.

- **Planes de mitigación:**

Intentar restablecer el sistema lo antes posible.

RIESGO 006. Falta de inversión

- **Descripción:**

No encontramos inversores que financian los costes de las recompensas.

- **Probabilidad:**

Verosímil.

- **Impacto:**

No habría tantas recompensas y quizá se perdería motivación por parte de los estudiantes anfitriones.

- **Indicadores:**

No hay financiadores de los premios.

- **Estrategias de prevención:**

Hacer un sistema atractivo para los inversores.

- **Planes de mitigación:**

Invertir en el proyecto de modo que, en caso de prosperar, este atrajese nuevos potenciales inversores.

RIESGO 007. Ofrecer lo mismo que la competencia

- **Descripción:**

Las empresas competidoras ofrecen lo mismo que nosotros.

- **Probabilidad:**

Muy probable.

- **Impacto:**

Al ofrecer todos un mismo producto o servicio, únicamente una de las empresas logrará hacerse con el control del mercado al atraer un mayor número de usuarios haciendo, de este modo, que el resto de aplicaciones caigan en desuso.

- **Indicadores:**

Análisis de aplicaciones similares a la nuestra.

- **Estrategias de prevención:**

Ofrecer servicios originales, únicos, difíciles de copiar.

- **Planes de mitigación:**

Reinventar alguna nueva funcionalidad.

RIESGO 008. Falta de interés durante el proyecto de parte del equipo de software

- **Descripción:**

Durante el curso de desarrollo del sistema, puede que algunos miembros del equipo de software pierdan el interés y abandonen el proyecto.

- **Probabilidad:**

Probable.

- **Impacto:**

Falta de miembros para seguir desarrollando el sistema y el consecuente aumento de los plazos.

- **Indicadores:**

Personal abandona el proyecto.

- **Estrategias de prevención:**

Pensar en un proyecto capaz de captar la atención de los miembros del equipo de desarrollo software y que resulte original y novedoso.

- **Planes de mitigación:**

Mantener motivado al personal.

RIESGO 009. No asistir al evento

- **Descripción:**

Un estudiante anfitrión pese a unirse a un evento acaba no asistiendo.

- **Probabilidad:**

Verosímil.

- **Impacto:**

El estudiante extranjero que haya creado el evento, contará con un participante menos, dando la situación que si el estudiante que no asiste era el único participante, no se pueda llevar a cabo la actividad.

- **Indicadores:**

El estudiante anfitrión no asiste al sitio de encuentro o tarda mucho en llegar y no ha comunicado el motivo por el cual llega tarde.

- **Estrategias de prevención:**

Penalización en forma de reducción del número de puntos si el estudiante no asiste al evento al cual se había unido, a no ser que sea por una causa justificada y se lo haya comunicado al estudiante que ha creado el evento. En caso de que un mismo estudiante no asistiese a múltiples eventos a los que se había unido en reiteradas ocasiones, se le impediría unirse a otros eventos durante un determinado periodo de tiempo.

- **Planes de mitigación:**

Advertir a los estudiantes que la falta asistencia, habiéndose unido previamente a un evento, llevará a cabo penalizaciones.