**FECHA DE ACTUALIZACIÓN**: 17 de abril del 2018

**ENCARGADO**: Mariana Mayorga Llano

# ORIGEN Y CRITERIO PARA AGRUPAR

El presente documento describe la lista de posibles riesgos que podrían presentarse en el proyecto y que podrían afectar el objetivo de la compañía. Dichos riesgos son clasificados y priorizados según la probabilidad de ocurrencia y el impacto que pueda causar en la empresa, su origen proviene del análisis de riesgo realizado por el personal.

# FRECUENCIA DE REVISIÓN DE RIESGOS

Se realizará un análisis de riesgos periódicamente cada año para añadir o modificar los riesgos actualizados. De la misma forma, el comité puede solicitar un nuevo análisis de riesgos en cualquier momento en caso de que lo consideren oportuno y necesario.

# MATRIZ DE RIESGOS

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Impacto** | **Probabilidad** | **Riesgo** | **Plan de acción** | |
| **Acceso de personal no autorizado a la información** | Muy alto | Alto | Severo | Reducir | Diseño arquitectónico enfocado en la seguridad, configuración de servidores y auditorías externas de seguridad.  En caso de ocurrencia se reestablecerán todos los permisos de usuario y se reforzará el control de acceso según se crea pertinente.  Se activará al inicio del proyecto en las fases de diseño e implementación, así como cada vez que se quiera hacer un cambio en componentes claves para la seguridad. |
| **Modificación no autorizada de la información** | Muy alto | Media | Severo | Reducir | Diseño arquitectónico enfocado en la seguridad, configuración de servidores y auditorías externas de seguridad.  En caso de ocurrencia se reestablecerán todos los permisos de usuario y se reforzará el control de acceso según se crea pertinente.  Se activará al inicio del proyecto en las fases de diseño e implementación, así como cada vez que se quiera hacer un cambio en componentes claves para la seguridad. |
| **Pérdida de información por daños de HW** | Muy alto | Baja | Mayor | Evitar | Respaldo de información constante en diferentes medios.  En caso de ocurrencia se intentará recuperar la información pero se registrará que dicha información no es la original y podría estar comprometida.  Se realizará periódicamente una vez al mes. |
| **Pérdida de información por daños de SW** | Muy alto | Muy baja | Moderado | Evitar | Respaldo de información constante en diferentes medios.  En caso de ocurrencia se intentará recuperar la información pero se registrará que dicha información no es la original y podría estar comprometida.  Se realizará periódicamente una vez al mes. |
| **Despliegue de información desactualizada o incorrecta** | Alto | Media | Mayor | Evitar | Control de versiones y actualización periódica de la información.  En caso de ocurrencia se realizará un análisis de las versiones y se establecerá y corregirá a la versión correcta.  Se activará cada vez que haya un cambio en el contenido del sistema. |
| **Pérdida de la conexión entre componentes internos** | Alto | Baja | Moderado | Evitar | Arquitectura de software enfocada a la disponibilidad con componentes redundantes.  En caso de ocurrencia se procederá a buscar una forma de reestablecer el servicio y posteriormente encontrar una solución definitiva al problema.  Se activará en el diseño de la arquitectura del sistema. |
| **Fallas en el registro de compras** | Muy alto | Alto | Severo | Evitar | Realización de pruebas, validación y verificación antes de la implementación de las funcionalidades o cambios.  En caso de ocurrencia se interrumpirá el servicio y se buscará una solución definitiva al problema para poder reestablecerlo.  Se realizará en la etapa de pruebas y verificación de funcionamiento del módulo. |
| **Inconsistencia en los registros** | Alto | Media | Mayor | Evitar | Control de versiones y actualización periódica de la información.  En caso de ocurrencia se realizará un análisis de las versiones y se establecerá y corregirá a la versión correcta.  Se activará cada vez que haya un cambio en el contenido del sistema. |
| **Desfasamiento en los tiempos de entrega** | Medio | Alta | Mayor | Reducir | Planificación de actividades y tareas.  En caso de ocurrencia se reestablecerá el calendario y la planificación tratando de adaptarse lo más posible a lo planeado.  Se activará al inicio del proyecto y se llevará a cabo hasta su finalización. |
| **Fallas en la integración de los componentes** | Muy alto | Alta | Severo | Evitar | Realización de pruebas, validación y verificación antes de la implementación de las funcionalidades o cambios.  En caso de ocurrencias el equipo técnico se encargara de buscar una solución temporal para reestablecer el servicio y posteriormente se buscará la solución definitiva.  Se realizará en la etapa de pruebas y verificación de funcionamiento del módulo. |

Orden de prioridades:

* Severos
* Mayores
* Moderado
* Baja

# SEGUIMIENTO A LA ACTIVACIÓN DEL PLAN DE ACCIÓN

Tras la implementación de un plan de acción para el manejo de un riesgo listado anteriormente se deberá realizar un reporte de las causas que llevaron a la implementación del mismo, las consecuencias y la evaluación del plan de acción junto con posibles mejoras en caso de que se requieran.