



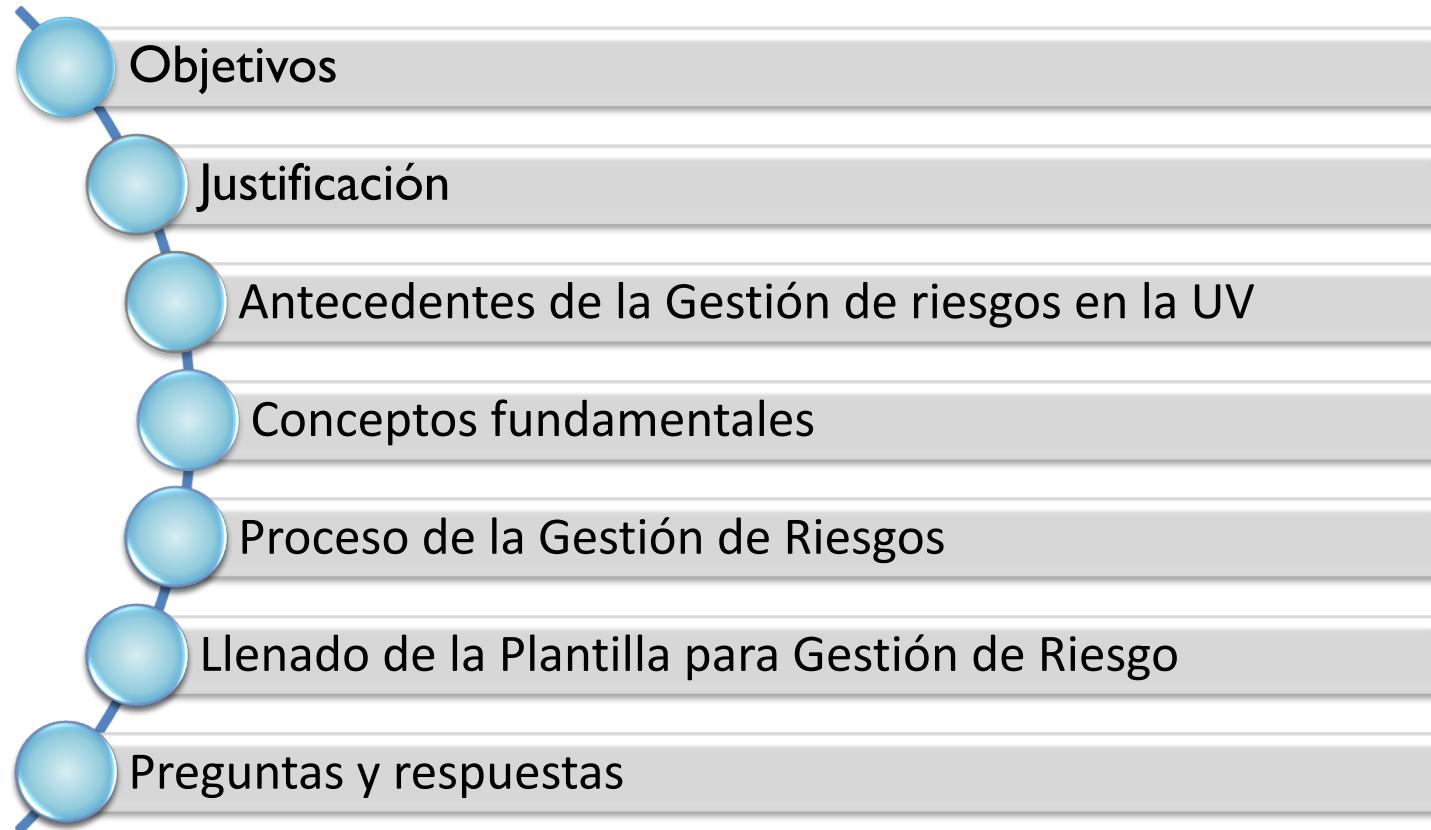
Universidad Veracruzana

Secretaría de Desarrollo Institucional
Dirección General de Tecnología de Información

Taller: Identificación y documentación de Riesgos asociados a los procesos establecidos en el alcance del SGCUV.

10 de Marzo de 2020

“Lis de Veracruz: Arte, Ciencia, Luz”



General

Identificar y documentar los riesgos asociados a los procesos establecidos en el alcance del Sistema de Gestión de la Calidad de la Universidad Veracruzana (SGCUV).

Específicos

- Identificar en sus procesos los riesgos que pudieran afectar negativamente el logro de los resultados previstos.
- Establecer una evaluación de los riesgos identificados y generar el plan de acción.
- Documentar los resultados del análisis de riesgo realizado, en la Plantilla de Gestión de Riesgos.

Durante la auditoría externa a los nuevos procesos que ampliaron el alcance del SGCUV en el mes de noviembre de 2019, se levantó una No Conformidad menor relativa a los riesgos:

- “Se identifican diferentes criterios para la determinación de los riesgos, en algunas matrices mencionan los riesgos, pero no se identifican los diferentes factores y por lo consiguiente, no se cuenta con planes de acción para los mismos.”
- “En otros casos, se colocaron solo los factores de los riesgos.”

Por lo anterior, este taller tiene la finalidad contribuir en la solución a esta no conformidad y reforzar el pensamiento basado en riesgos.

- 2012. Derivado de la Ley 581 para la tutela de los datos personales en el estado de Veracruz, se iniciaron actividades para la implementación de un Sistema de Gestión de Seguridad de la Información el cual exige la elaboración de un análisis de riesgos.
- 2013. DGTI desarrolló una metodología y plantilla para la gestión de riesgos basada en la ISO 27005 y Magerit.
- 2018. Se crea el Comité de Control Interno y Desempeño Institucional(COCODI) con el objetivo de establecer estrategias y líneas de acción para crear, actualizar y evaluar en forma permanente y sistemática el ambiente de control interno institucional, para contribuir al cumplimiento oportuno de metas y objetivos con enfoque a resultados, fomentando una cultura de respeto a la legalidad, conducta ética, responsabilidad social, disciplina, objetividad, profesionalismo, honradez, lealtad, imparcialidad, integridad, rendición de cuentas, eficacia, eficiencia, principios y directrices que deben regir el servicio público.
- 2018. En el COCODI se crea el Grupo de trabajo sobre la Administración de Riesgos (GTAR), quién, en coordinación con la DGTI, elaboró un Manual para la identificación y evaluación de Riesgos en la UV y las actualizaciones correspondientes a la plantilla.

- 2019. Se imparte el **Taller para el llenado de la plantilla de gestión de riesgos** dirigido al personal que participa en los nuevos procesos y subprocesos que se incorporan al SGCUV.
- 2019. Se imparte el taller: **Control interno y Administración de Riesgos** con el objetivo de aplicar las etapas de la Administración de Riesgos de conformidad con la Metodología de la Entidad acorde al Marco Integrado de Control Interno.
- 2019. Elaboración de 18 matrices de riesgo, 16 corresponden a dependencias con procesos declarados en el alcance del SGCUV y 2 declarados como susceptibles al riesgo de corrupción (www.uv.mx/cocodi).
- 2020.
 - Febrero. Se imparte el curso **Control Interno y Administración de Riesgos** en la Región Veracruz
 - Marzo. Se impartirá el mismo curso en la Región Orizaba-Córdoba

Debido a que convergen los temas, la pretensión es lograr que la Institución utilice la misma metodología tanto para el análisis de riesgos institucionales, como los que se requieran por proceso.

Riesgo

Es un evento adverso e incierto (interno o externo) que derivado de la combinación de la **probabilidad** de ocurrencia y el posible **impacto**, al materializarse pudiera impedir u obstaculizar el logro de los objetivos y metas institucionales.

Factor de Riesgo

Se refiere a una situación, estado, circunstancia (interna o externa) o cualquier elemento que pudieran dar lugar a que se incremente la probabilidad de que se materialice un Riesgo.

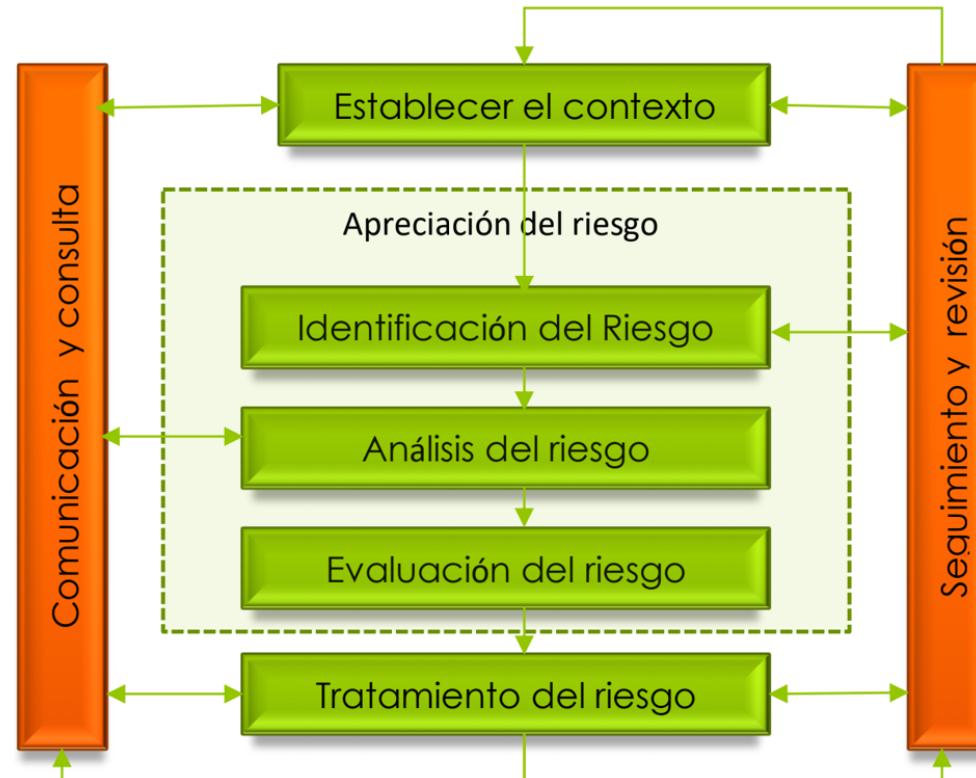
Control

Medida que modifica un riesgo. Incluyen cualquier proceso, política, dispositivo, práctica,. Un control debe ser *Existente, Suficiente y Eficiente*.

Riesgo residual

Riesgo remante después del tratamiento del riesgo (proceso destinado a modificar el riesgo)

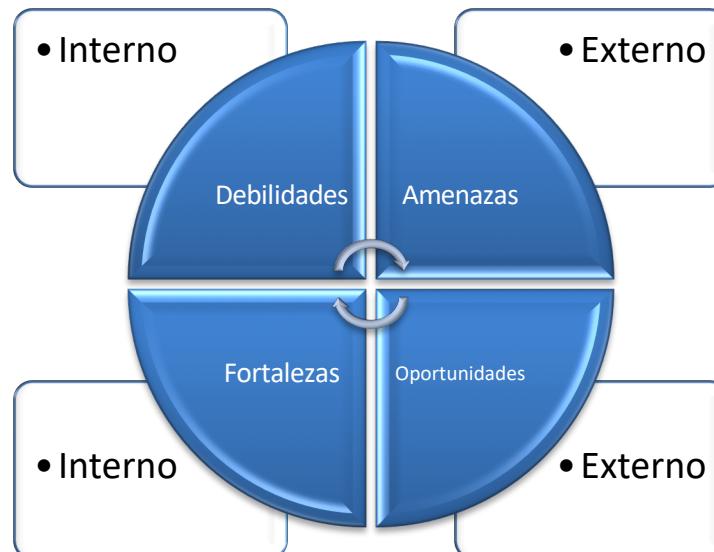
Proceso de la Gestión de Riesgos



Establecer el contexto

Situaciones Intrínsecas:

- Estructura
- Funciones/atribuciones
- Procesos/productos
- Objetivos/Estrategias
- Recursos Humanos
- Recursos Financieros
- Tecnología de la Información



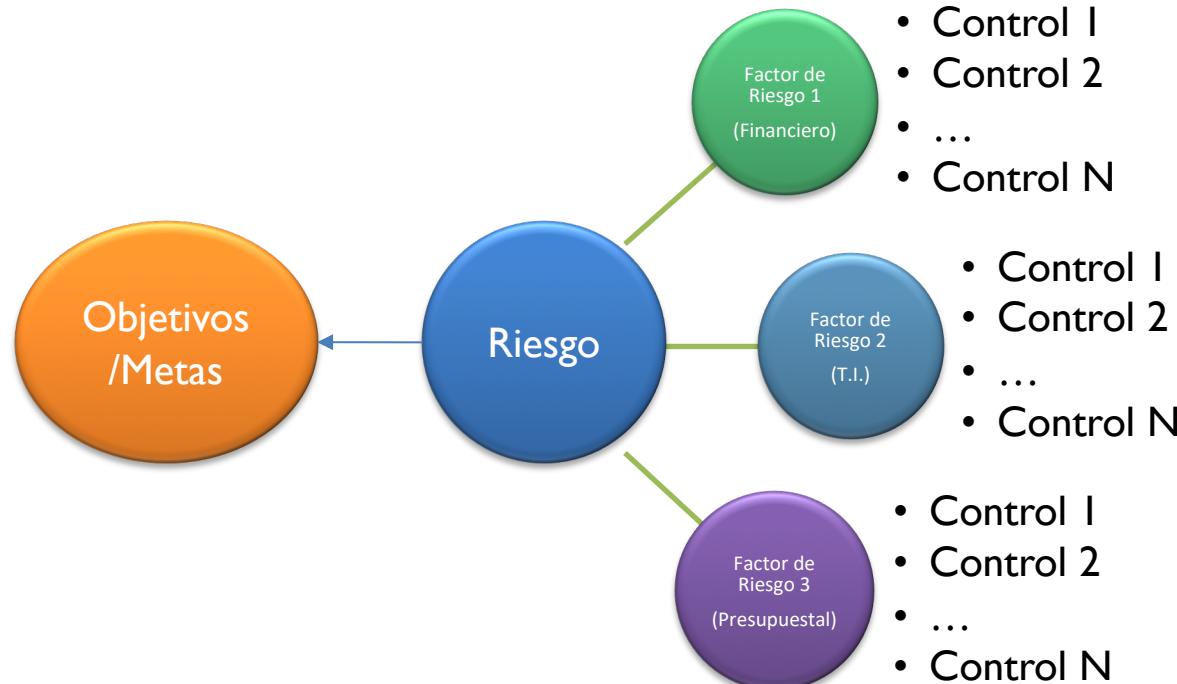
Internacional, nacional y/o regional:

- Social
- Política
- Legal
- Financiera
- Tecnológica
- Económica
- Ambiental



Identificación del riesgo

Condición indispensable para la identificación de los riesgos: **Conocer los objetivos o metas.**



Identificación del riesgo

El **nivel de decisión del riesgo** puede ser:

- **Estratégico**
Logro de misión, visión, objetivos y metas institucionales
- **Directivo o Táctico**
Relativo a la operación de los procesos o programas
- **Operativo**
La ejecución de las tareas de los procesos o procedimientos se lleven a cabo de manera efectiva y eficiente

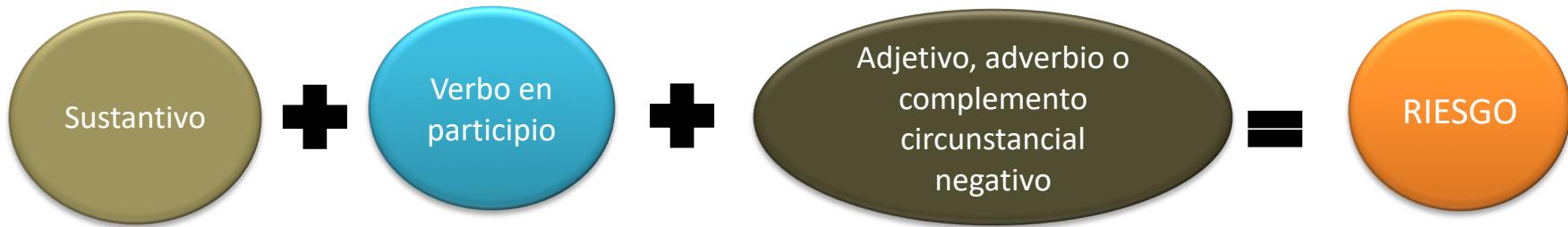
Proceso de la Gestión de Riesgos

Identificación del riesgo

Universidad Veracruzana



Identificación del riesgo: Estructura de redacción



Administrar = administrado
Realizar = realizado, realizadas
Controlar = Controlado

Ejemplos de redacción del riesgo

Sustantivo	Verbo participativo	Adjetivo, adverbio o complemento circunstancial negativo	Riesgo
Compras	Realizadas	Sin la calidad requerida o incumplimiento de requisitos legales establecidos	Compras realizadas sin la calidad requerida o incumplimiento de requisitos legales establecidos
Presupuesto de proyectos internos y externos	Administrado	Deficientemente	Presupuesto de proyectos internos y externos administrados deficientemente
Equipo de cómputo y periférico	Dictaminado	erróneamente	Equipo de cómputo y periférico dictaminado erróneamente
Sanciones	Aplicadas	por el órgano garante por falta de aplicación de niveles de seguridad al sistema de datos personales	Sanciones aplicadas por el órgano garante por falta de aplicación de niveles de seguridad al sistema de datos personales
Sala de Juntas	Prestada	Erróneamente por una mala gestión	Sala prestada erróneamente por una mala gestión



Análisis y evaluación del riesgo

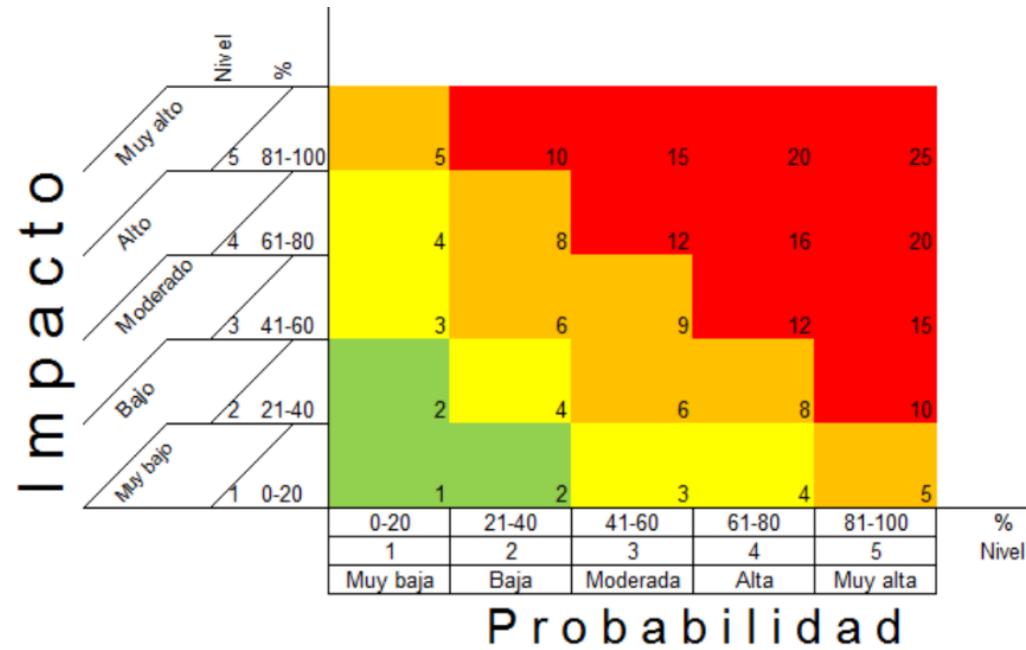
Nivel	Término	Descripción
1	Muy baja	El riesgo puede ocurrir con una probabilidad del 20% o menos
2	Baja	El riesgo puede ocurrir con una probabilidad entre el 21% y el 40%
3	Moderada	El riesgo puede ocurrir con una probabilidad entre el 41% y el 60%
4	Alta	El riesgo puede ocurrir con una probabilidad entre el 61% y el 80%
5	Muy Alta	El riesgo puede ocurrir con una probabilidad del 81% o más

Probabilidad de ocurrencia

Nivel	Término	Descripción del impacto
1	Muy bajo	Sólo causa incomodidad leve pero manejable, si el hecho llegara a presentarse degradaría el proceso, producto o servicio o tendría efectos mínimos en la institución.
2	Bajo	Sólo causa incomodidad que se debe atender pero no afecta la funcionalidad del proceso, producto o servicio, tendría bajo impacto en la institución.
3	Moderado	Disminuye el desempeño del proceso, producto o servicio y tendría medianas consecuencias o efectos en la institución.
4	Alto	Afecta el proceso, producto o servicio, tendría fuertes consecuencias o efectos en la institución.
5	Muy alto	Detiene el proceso, producto o servicio y tendría desastrosas consecuencias en la institución.

Impacto

Análisis y evaluación del riesgo: Mapa de calor



Análisis y evaluación del riesgo

Factores y controles del riesgo

- Establecer las posibles consecuencias que traería consigo, la materialización del riesgo, especificando las afectaciones negativas a las metas, objetivos, productos, servicios, procesos, etc., según sea el caso.
- Establecer/documentar los controles existentes: preventivo o correctivo. Su grado de eficiencia y eficacia del control para administrar el riesgo.
- Realizar un análisis para determinar la pertinencia y viabilidad financiera, técnica y de operación en la implementación de los controles.



Tratamiento del Riesgo

Una vez que se tienen documentados los controles se debe de valorar si están:

- Documentados;
- Formalizados;
- Son aplicados;
- Son eficientes.

De acuerdo a la valoración obtenida se determina que estos controles son:

- Eficientes/Suficientes. La valoración del riesgo pasa a una escala inferior. El desplazamiento depende de si el control incide en el impacto y/o la probabilidad;
- Deficientes/inexistentes. Se mantiene el resultado de la valoración del riesgo antes de controles.

Tratamiento del Riesgo

Posterior a la evaluación inicial del riesgo y a la implementación de controles, se debe valorar nuevamente el impacto y probabilidad de ocurrencia del riesgo, lo que permite visualizar en el mapa de calor en que cuadrante se encuentra el riesgo para determinar que acción aplicar.

- Aceptar / Asumir;
- Mitigar / Reducir;
- Transferir, o
- Evitar.

Tratamiento del Riesgo

Riesgo	Observación	Decisión
Bajo	Las medidas o acciones establecidas son efectivas y están documentadas, se acepta el riesgo potencial con documentación de soporte. Esta estrategia deberá usarse sólo para riesgos de bajo impacto y baja probabilidad de ocurrencia.	Aceptar/ Asumir
Moderado	El riesgo ha sido identificado y representa una amenaza para el cumplimiento de los objetivos, proceso, productos o servicios, por lo que se deben establecer acciones dirigidas a disminuir la probabilidad de ocurrencia y el impacto.	Mitigar/ Reducir
Alto	<p>Las medidas o acciones existentes no son efectivas, se deben fortalecer o compartir mediante la asignación de responsabilidades o contratación de seguros. Consiste en trasladar el riesgo mediante la responsabilidad de un tercero (tercerización especializada), la cual cuenta con las tres dimensiones siguientes:</p> <ul style="list-style-type: none">➤ Protección o cobertura: La acción que se realiza para reducir la posibilidad de una pérdida, obliga también a renunciar a la posibilidad de una ganancia.➤ Aseguramiento: Significa pagar una prima (el precio del seguro) para que en caso de tener pérdidas estas sean asumidas por la aseguradora.➤ Diversificación: Implica mantener cantidades similares de muchos activos riesgosos en lugar de concentrar toda la inversión en uno sólo producto.	Transferir
Muy alto	Las medidas o acciones no existen, se deberá realizar atención inmediata para eliminar el factor o los factores que podrían provocar el riesgo.	Evitar

Llenado de la plantilla para gestión de riesgos

Universidad Veracruzana



Proceso Nivel I

Identificar los procesos del alcance del SGC-UV

01



Proceso Nivel 2 (SubProcesos)

Identificar los subprocesos de cada proceso del SGC-UV

02



Proceso Nivel 3 (Procedimientos)

Identificar los procesos Nivel 3 de cada proceso nivel 2 y 3

03



Acciones

Identificar las acciones aplicar (evitarlo, mitigarlo, aceptarlo)

04



Factor del Riesgo (Disparador o síntoma)

Identificar los factores que detonan el riesgo (leyes, reglamentos, fallas, auditorías)

05



Categorías

Identificar las categorías de cada riesgo (Recurso humano, técnicos, TIC's, Servicio)

06



Riesgos

Identificar los riesgos asociados a cada proceso

07



Gestión del Riesgo



Visualizar los riesgos evaluados



Mapa de Calor del Riesgo

Preguntas

