GESTION DE PROYECTOS INFORMATICOS –2025 - I

Dr. Cayo Leon Fernandez
Profesor Principal – FISI
Consultor en TI

Grupo de proceso de Planificacion

Area de Conocimiento de Riesgos

Planificando el Proyecto

Áreas del Conocimiento	GRUPO DE PROCESOS DE DIRECCIÓN DE PROYECTOS				
	Grupo de Procesos de Iniciación	Grupo de Procesos de Planificación	Grupo de Procesos de Ejecución	Grupo de Procesos de Seguimiento y Control	Grupo de Procesos de Cierre
Gestión de la Integración del Proyecto	• Desarrollar el acta de constitución del proyecto • Desarrollar el enunciado preliminar del alcance del proyecto	• Desarrollar el plan de gestión del proyecto	• Dirigir y gestionar la ejecución del proyecto	• Supervisar y controlar el trabajo del proyecto • Control integrado de cambios	• Cerrar proyecto
Gestión del Alcance del Proyecto		• Planificar el alcance • Definir el alcance • Crear EDT		• Verificar el alcance • Controlar el alcance	
Gestión del Tiempo del Proyecto		• Definir las actividades • Establecer la secuencia de actividades • Estimar los recursos de las actividades • Estimar la duración de las actividades • Desarrollar el cronograma		• Controlar el cronograma	
Gestión de Costos del Proyecto		• Estimar los costos • Preparar el presupuesto de costos		• Controlar los costos	
Gestión de la Calidad del Proyecto		• Planificación de la calidad	• Realizar el aseguramiento de calidad	• Controlar la calidad	
Gestión de los RR.HH del Proyecto		• Planificación de los RR.HH	• Adquirir el equipo del proyecto • Desarrollar el equipo del proyecto	• Gestionar el equipo del proyecto	
Gestión de las comunicaciones del Proyecto		• Planificación de las comunicaciones	• Distribuir la información	• Informar el rendimiento • Gestionar a los interesados	
Gestión de los riesgos del Proyecto		• Planificación de la gestión de riesgos • Identificar los riesgos • Analizar cualitativamente • Analizar cuantitativamente • Planificar la respuesta a los riesgos		• Seguir y controlar los riesgos	
Gestión de las adquisiciones del Proyecto		• Planificar las compras y adquisiciones • Planificar el contrato	• Solicitar respuestas de los vendedores • Seleccionar vendedores	• Administrar el contrato	• Cerrar contrato

Planificar la Gestión de Riesgos

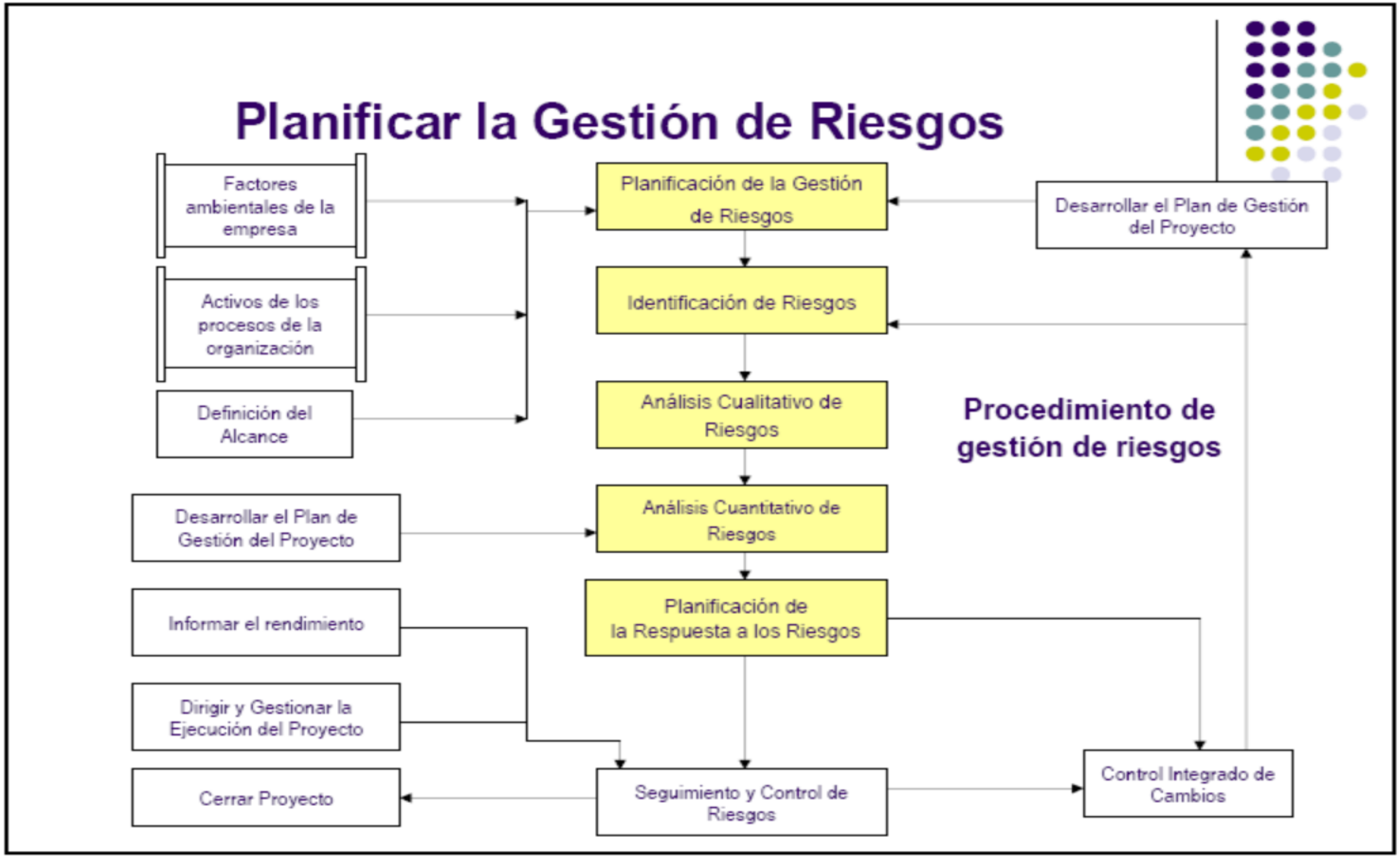
Un Riesgo (Risk) de un proyecto es un evento o condición inciertos que, si se produce, tiene un efecto positivo o negativo sobre al menos un objetivo del proyecto, como tiempo, costo, alcance o calidad (es decir, cuando el objetivo de tiempo de un proyecto es cumplir con el cronograma acordado; cuando el objetivo de costo del proyecto es cumplir con el costo acordado, etc.).

El riesgo de un Proyecto tiene su origen en la incertidumbre que está presente en todos los proyectos. Riesgos conocidos son todos aquellos que han sido identificados y analizados, y es posible planificar dichos riesgos siguiendo los procesos de Gestión de Riesgos. Los riesgos desconocidos no pueden gestionarse proactivamente, y una respuesta prudente del equipo del proyecto puede ser asignar una contingencia general contra dichos riesgos, así como contra riesgos conocidos para los cuales quizá no sea rentable o posible desarrollar respuestas proactivas.

El Proceso de Planificación de la Gestión del Riesgo incluye adoptar las siguientes acciones:

- Identificar el riesgo.
- Analizar el riesgo.
- Evaluar el Riesgo (Cuantificar - Cualificar)
- Planes de Acción (Estrategia para minimizar los riesgos).
- Contingencia.

Planificar la Gestión de Riesgos



Planificar la Gestión de Riesgos

El **RBS (Risk Breakdown Structure: Estructura de Desglose de Riesgos)** es la descomposición de todos los posibles riesgos que se han identificado durante el proceso de Planificación.

Nos va a permitir visualizar objetivamente el alcance de todos los riesgos asistentes y su impacto en el proyecto.

RBS: Estructura de Desglose de Riesgos

Ejemplo

Planificar la Gestión de los Riesgos

Entradas	Herramientas y Técnicas	Salidas
.1 Factores ambientales de la empresa .2 Activos de los procesos de la organización .3 Enunciado del alcance del proyecto .4 Plan de gestión del proyecto	.1 Reuniones y análisis de planificación	.1 Plan de gestión de riesgos

- **Metodología.**
- **Roles y responsabilidades.**
- **Preparación del presupuesto.**
- **Periodicidad.**
- **Categorías de Riesgo.**
- **Definiciones de Probabilidad e Impacto de los Riesgos.**
- **Matriz de Probabilidad e Impacto.**
- **Tolerancia revisadas de los interesados.**
- **Formatos de Informe.**
- **Seguimiento.**

Planificar la Gestión de los Riesgos

Plan de gestión de riesgos (Continuación)

• **Categorías de riesgo**. Proporciona una estructura que garantiza un proceso completo de identificación sistemática de los riesgos con un nivel de detalle uniforme, y contribuye a la efectividad y calidad de la Identificación de Riesgos. Una estructura de desglose del riesgo (**Risk Breakdown Structure: RBS**) es uno de los métodos para proporcionar dicha estructura, pero también se puede utilizar un listado de los diversos aspectos del proyecto.

RBS: Estructura de Desglose de Riesgos

Planificar la Gestión de los Riesgos

Plan de gestión de riesgos (Continuación)

- **Matriz de probabilidad e impacto**. Los riesgos se priorizan según sus posibles implicaciones para lograr los objetivos del proyecto. El método típico para priorizar los riesgos es utilizar una tabla de búsqueda o una Matriz de Probabilidad e Impacto (véase Herramientas y Técnicas de Analizar Cualitativamente los riesgos).
- **Tolerancias revisadas de los interesados**. Las tolerancias de los interesados pueden revisarse en el proceso Planificación de la Gestión de Riesgos, ya que se aplican al proyecto específico.
- **Formatos de informe**. Describe el contenido y el formato del registro de riesgos, así como de cualquier otro informe de riesgos que se requiera. Define cómo se documentarán, analizarán y comunicarán los resultados de los procesos de gestión de riesgos.
- **Seguimiento**. Documenta cómo todas las facetas de las actividades de riesgo serán registradas para beneficio del proyecto actual, para futuras necesidades y para las lecciones aprendidas. Documenta si serán auditados los procesos de gestión de riesgos y cómo se realizaría dicha auditoria.

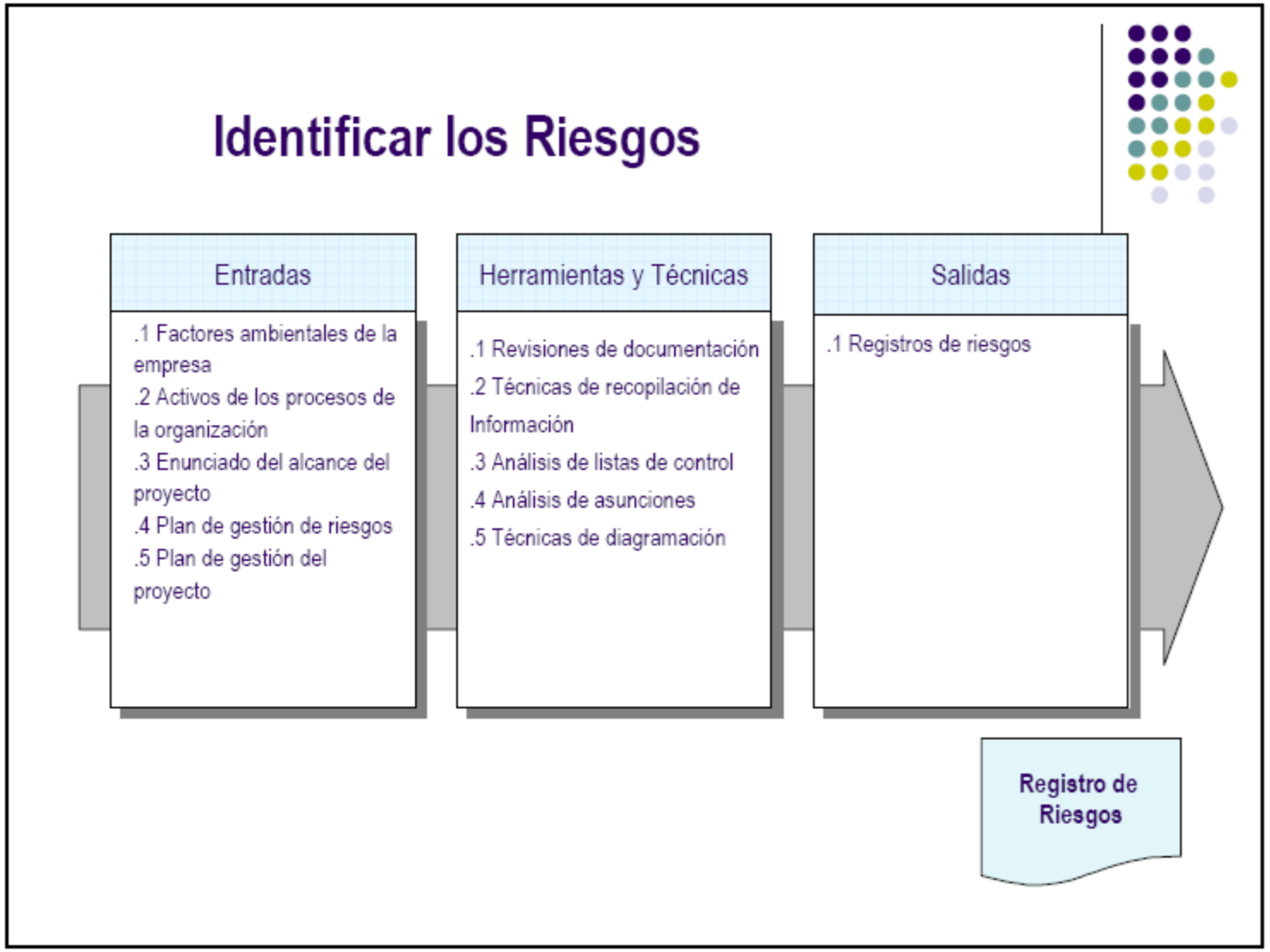
Teoria de la utilidad

Identificar los Riesgos

Consiste en determinar que riesgos pueden afectar al proyecto y documentar sus características.

Nr	Descripción del riesgos	Categoría	Probab.	Impacto	Severidad	Respons.	Respuesta	Disparador	Contingencia
1	Poca disponibilidad de recursos de los participantes del proyecto	Personal						Sobrecarga horaria	
2	Poco tiempo para la culminación del Proyecto	Tiempo						Desviaciones fecha > 5%	
3	Salida del personal por trabajo o practica	Personal						Salida del personal	
4	Poca experiencia del personal puede afectar la calidad de los productos	Personal						Errores encontrados	

Ejemplo


Identificar los Riesgos
Entradas
.1 Factores ambientales de la empresa
.2 Activos de los procesos de la organización
.3 Enunciado del alcance del proyecto
.4 Plan de gestión de riesgos
.5 Plan de gestión del proyecto
Herramientas y Técnicas
.1 Revisiones de documentación
.2 Técnicas de recopilación de Información
.3 Análisis de listas de control
.4 Análisis de asunciones
.5 Técnicas de diagramación
Salidas
.1 Registros de riesgos
Registro de Riesgos

Identificar los Riesgos

Salidas

.1 Registros de riesgos.

El registro de riesgos contiene los resultados de los demás procesos de gestión de riesgos a medida que se llevan a cabo. La preparación del registro de riesgos comienza en el proceso Identificación de Riesgos, y luego está disponible para la gestión de otros proyectos y otros procesos de Gestión de los Riesgos del Proyecto.

- Lista de riesgos identificados.
- Lista de posibles respuestas.
- Causas de los riesgos.
- Categorías de riesgo actualizadas.

Analizar Cualitativamente los riesgos

Consiste en realizar un análisis cualitativo de la probabilidad y el impacto de los riesgos principalmente con el objetivo de priorizarlos por su severidad

Nr	Descripción del riesgos	Categoría	Probab.	Impacto	Severidad	Responsable	Respuesta	Disparador	Contingencia
1	Poca disponibilidad de recursos de los participantes del proyecto	Personal	0.5	1	0.5			Sobrecarga horaria	
2	Poco tiempo para la culminación del Proyecto	Tiempo	0.2	2	0.4			Desviaciones fecha > 5%	
3	Salida del personal por trabajo o practica	Personal	0.5	3	1.5			Salida del personal	
4	Poca experiencia del personal puede afectar la calidad de los productos	Personal	0.5	3	1.5			Errores encontrados	

Ejemplo

Criterios de evaluación de riesgos

Para la evaluación de riesgos se utilizarán, como valores primarios, la calificación de impacto y probabilidad de cada riesgo.

Para ambos casos se utilizarán tablas de 5 valores con las equivalencias que se señalan a continuación.

A partir de esos valores se calculará el nivel de exposición y la severidad de los riesgos representándolos en el mapa térmico.

Calificación de la probabilidad

Para la calificar la probabilidad de los riesgos se utilizará una tabla de 5 valores:

Probabilidad	
P	**Significado**
5	Casi seguro
4	Muy probable
3	Probable
2	Poco probable
1	Raro

Calificación del impacto

Para calificar el impacto se utilizará una tabla general de referencia con 5 valores; adicionalmente se utilizarán tablas específicas donde se describirán los criterios para asignar la calificación de impacto según la categoría de cada riesgo:

Impacto	
I	Significado
5	Mayor
4	Importante
3	Significativo
2	Regular
1	Menor

Severidad del riesgo

Para medir la severidad del riesgo se utilizarán 4 valores que se determina según la calificación del impacto y la probabilidad, es decir el nivel de exposición:

Severidad	
S	Significado
4	Extrema
3	Alta
2	Moderada
1	Baja

Mapa térmico

En la siguiente tabla se presenta el modelo para el mapa térmico donde según la calificación de impacto y probabilidad el riesgo es calificado por color en su nivel de severidad. El color rojo representa severidad extrema, el color naranja severidad alta, el color amarillo claro severidad moderada y el color verde claro severidad baja:

Impacto	1	2	3	4	5
5	M	A	E	E	E
4	M	A	A	E	E
3	B	M	A	A	E
2	B	M	M	A	A
1	B	B	B	M	M
	1	2	3	4	5
	Probabilidad				

Categorías de los riesgos

Categoría	Descripción
Gestión	Riesgos relacionados con la ausencia o aplicación incorrecta de métodos de gestión de las tecnologías de información y comunicaciones.
Operación	Incumplimiento de directrices, procedimientos y metodologías y estándares en los procesos operativos de la UTI.
Infraestructura	Riesgos relacionados con las fallas potenciales de la infraestructura tecnológica utilizada en la CGR.
Seguridad	Eventos que atentan contra la confidencialidad, integridad y disponibilidad de la información.
Recurso humano	Relacionados con el desempeño y regularidad de los recursos humanos.

Identificación de riesgos

Id	Descripción del Riesgo	Categoría
1	Adquisición de soluciones automatizadas que no satisfagan las necesidades de la institución.	Gestión
2	Desarrollar productos que no cumplen con las especificaciones.	Gestión
3	Desarrollar productos basados en requerimientos incorrectos.	Gestión
4	Versiones de software desactualizadas.	Gestión
5	Adquirir software sin programas fuentes.	Gestión
6	Adquirir software que no tiene representación en el país.	Gestión
7	Equipo dañado no puede ser reparado.	Operación
8	Red inalámbrica insegura.	Operación
9	Daño físico en los equipos de la plataforma tecnológica.	Operación
10	Obsolescencia de la infraestructura tecnológica.	Gestión
11	Desarrollo de sistemas y servicios que son difíciles de utilizar para el usuario.	Gestión

Identificación de riesgos

Id	Descripción del Riesgo	Categoría
12	No existe guía de usuario para el uso del sistema.	Gestión
13	Retrasos en los procesos de contratación administrativa.	Gestión
14	Se adquiere equipo no compatible con la infraestructura en uso.	Gestión
15	Se adquiere equipo sin que existan talleres para la reparación y mantenimiento de los mismos.	Gestión
16	Trabajar directamente en equipos de producción.	Operación
17	Versiones de software para desarrollo y producción diferentes.	Operación
18	No contar con la metodología y procedimientos necesarios para la administración de los cambios.	Operación
19	Libertad en el uso de componentes tecnológicos (software libre).	Gestión
20	Instalación de parches sin seguir las recomendaciones del proveedor.	Operación
21	Ausencia de niveles de servicio aceptados que faciliten la gestión.	Gestión

Identificación de riesgos

Id	Descripción del Riesgo	Categoría
22	Definición de niveles de servicio que sobrepasan la capacidad instalada de TI.	Gestión
23	No contar con los recursos necesarios para cumplir con los niveles de servicio.	Gestión
24	No existe contrato de mantenimiento	Gestión
25	Debilidad en la administración de servicios de terceros que implica que éstos no cumplan satisfactoriamente los requerimientos del negocio.	Gestión
26	Incumplimiento de las políticas definidas por las partes.	Gestión
27	Tiempo de respuesta degradado.	Operación
28	No hacer planeamiento de la capacidad.	Gestión
29	Los recursos de la infraestructura tecnológica no son suficientes para atender las demandas de servicios.	Gestión
30	Recuperación de software no es factible	Operación
31	Suspensión de servicio de Internet	Infraestructura
32	Fallas en los equipos de comunicaciones	Infraestructura
33	Fallas en los servidores (computadores principales)	Infraestructura
34	Equipo de usuario final inseguro.	Seguridad

Identificación de riesgos

Id	Descripción del Riesgo	Categoría
35	Ausencia de controles cruzados que comprueben la integridad de la información y el funcionamiento correcto de las aplicaciones.	Seguridad
36	Errores en la creación de usuarios y en la asignación de privilegios de acceso.	Seguridad
37	Sistemas sin mecanismos de trazabilidad de transacciones (pistas de auditoría).	Seguridad
38	No se conocen los costos asignados a los servicios prestados por TI.	Gestión
39	No se cuenta con un proceso de análisis para mejorar los costos que están asociados a los servicios de TI.	Gestión
40	El personal no cuenta con el tiempo suficiente para recibir, de manera completa, la capacitación correspondiente.	Gestión
41	El personal no cuenta con las actitudes y aptitudes requeridas para hacer uso de la información por medio de las soluciones automatizadas.	RRHH

Identificación de riesgos

Id	Descripción del Riesgo	Categoría
42	La capacitación que se brinda a los usuarios no es efectiva para que puedan utilizar eficientemente los recursos informáticos disponibles.	Gestión
43	No se cuenta con presupuesto para diseñar e implementar programas de capacitación para los usuarios.	Gestión
44	No contar con una respuesta oportuna y efectiva para las consultas de los usuarios de TI y a la atención de los incidentes.	Operación
45	Las soluciones que se aplican, ante los incidentes reportados por los usuarios, no son efectivas.	Operación
46	Los usuarios no están informados sobre los procedimientos que se deben seguir para reportar los incidentes.	Gestión
47	No se cuenta o no se aplica el procedimiento definido para la asignación, atención y seguimiento de los incidentes.	Operación
48	No se realiza una adecuada gestión de métricas sobre los incidentes reportados y atendidos.	Gestión

Identificación de riesgos

Id	Descripción del Riesgo	Categoría
49	Se realizan cambios operativos que no se reflejan en la documentación.	Operación
50	Se realizan cambios en la configuración de componentes de la infraestructura y no se reflejan en la documentación.	Operación
51	No se conoce el impacto de hacer cambios en los componentes de la configuración.	Operación
52	No se aplica el procedimiento oficializado para la gestión de problemas.	Operación
53	No se documentan las soluciones aplicadas a los problemas.	Operación
54	Hay dificultad para definir el ámbito de acción de los proveedores para la solución de problemas.	Gestión
55	Alteración o pérdida de la información registrada en base de datos o equipos.	Seguridad
56	Información desactualizada o incorrecta.	Operación
57	Acceso no autorizado a la información.	Seguridad
58	Instalaciones físicas mal diseñas que pongan en peligro la integridad del equipo de cómputo y del personal.	Gestión
59	Acceso no autorizado al centro de cómputo.	Seguridad

Identificación de riesgos

Id	Descripción del Riesgo	Categoría
60	Ausencia de detectores de humo.	Seguridad
61	Fallas en los equipos que mantienen el medio ambiente apropiado para la operación de TI (UPS, Aire acondicionado)	Infraestructura
62	No aplicación de las políticas para la generación de respaldos.	Operación
63	No efectuar un monitoreo constante sobre la operación de la plataforma.	Operación
64	Suspensión de servicios sin seguir el procedimiento establecido.	Operación
65	No contar con un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI.	Gestión
66	No percibir los cambios que se realizan en el entorno.	Gestión
67	Utilización de indicadores sobre el desempeño de TI que no son relevantes y que no colaboran en la identificación de oportunidades de mejora en los procesos importantes de TI.	Gestión

Identificación de riesgos

Id	Descripción del Riesgo	Categoría
68	No contar con un programa de control interno efectivo para TI que incluya auto-evaluaciones y revisiones por parte de terceros.	Gestión
69	No contar con la documentación de los procesos de TI.	Gestión
70	Uso de software no licenciado	Seguridad
71	Exceder la cantidad de usuarios autorizados para utilizar un producto licenciado.	Operación
72	Facilitar los medios para la instalación de software a terceros.	Operación
73	Contar con un plan estratégico no alineado a la estrategia institucional.	Gestión
74	Se tiene Plan Estratégico desactualizado.	Gestión
75	No contar con un modelo de información del negocio que sea utilizado en la creación y actualización de los sistemas de información.	Gestión
76	Arquitectura de información desactualizada.	Gestión

Identificación de riesgos

Id	Descripción del Riesgo	Categoría
77	Arquitectura de información no responde a la cadena de valor.	Gestión
78	Adquisición de tecnologías que no aportan valor a la organización.	Gestión
79	Contar con equipo costoso que no cuenta con contratos de mantenimiento.	Gestión
80	No aplicación de los canales de comunicación establecidos para informar sobre la gestión de TI.	Gestión
81	No se tienen documentados los canales de comunicación.	Gestión
82	No se tiene dominio sobre las herramientas en uso.	RRHH
83	Equipo de trabajo con baja motivación, poco creativo y no comprometido con el logro de los objetivos.	RRHH
84	Contar con un sistema de administración de la calidad deficiente en la definición y aplicación de procesos y procedimientos para el desarrollo de las TIC en la institución.	Operación
85	Desarrollar productos que no cumplen con los requerimientos de calidad.	Operación
86	No administrar los riesgos de TI.	Gestión

Identificación de riesgos

Id	Descripción del Riesgo	Categoría
87	Utilizar un marco de trabajo deficiente para la gestión de riesgos, y no alineado con el apetito del riesgo institucional.	Gestión
88	El personal no está capacitado adecuadamente para realizar una gestión efectiva de los riesgos.	Gestión
89	No contar con el contenido presupuestario para la ejecución de los proyectos.	Gestión
90	Inestabilidad en el equipo de proyecto.	Gestión
91	Desarrollo de proyectos no alineados al Plan Estratégico	Gestión
92	Los proyectos no están documentados	Gestión
93	No contar con un marco de referencia para la gestión de los proyectos en cuanto a su iniciación, planificación, ejecución, control y cierre, o aplicar ese marco de referencia deficientemente.	Gestión
94	Exceder el tiempo planificado para la ejecución de los proyectos.	Gestión
95	Falta de apoyo del patrocinador del proyecto.	Gestión

Identificación de causas

Cada uno de los riesgos identificados está asociado con una o varias causas, conocer las causas es importante para enfocar los posteriores esfuerzos de mitigación y contingencia así como para calificar los controles existentes. Las causas asociadas a cada riesgo identificado son las siguientes:

Id	Descripción del riesgo	Causas
1	Adquisición de soluciones automatizadas que no satisfagan las necesidades de la institución.	Especificación de requerimientos no adecuada. No se validó el cumplimiento del producto.
2	Desarrollar productos que no cumplen con las especificaciones.	Errores de concepto al analizar las especificaciones No se validaron los componentes del producto

Evaluación de riesgos

Evaluación de riesgos absolutos

La primera evaluación corresponde a los riesgos absolutos, es decir, valorar el nivel de severidad de cada riesgo sin tomar en cuenta el efecto de los controles que se aplican actualmente.

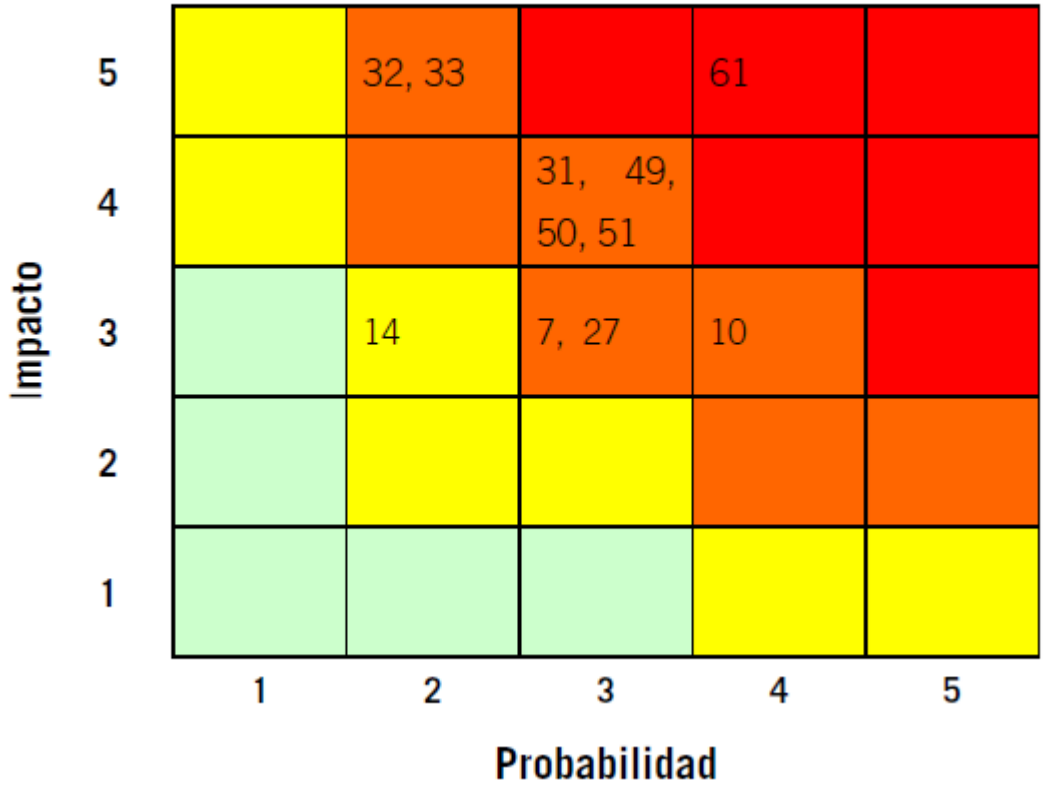
Como fue definido anteriormente, la calificación se realiza utilizando dos criterios primarios que son la probabilidad (P) y el impacto (I) de cada riesgo, de esto valores se deriva el nivel de exposición (**P * I**) y la severidad de los riesgos

Id	Riesgo	P	I	S
1	Adquisición de soluciones automatizadas que no satisfagan las necesidades de la institución.	3	3	9
2	Desarrollar productos que no cumplen con las especificaciones.	2	4	8
3	Desarrollar productos basados en requerimientos incorrectos.	2	4	8
4	Versiones de software desactualizadas.	3	4	12
5	Adquirir software sin programas fuentes.	1	4	4
6	Adquirir software que no tiene representación en el país.	1	4	4
7	Equipo dañado no puede ser reparado.	3	3	9
8	Red inalámbrica insegura.	5	5	25

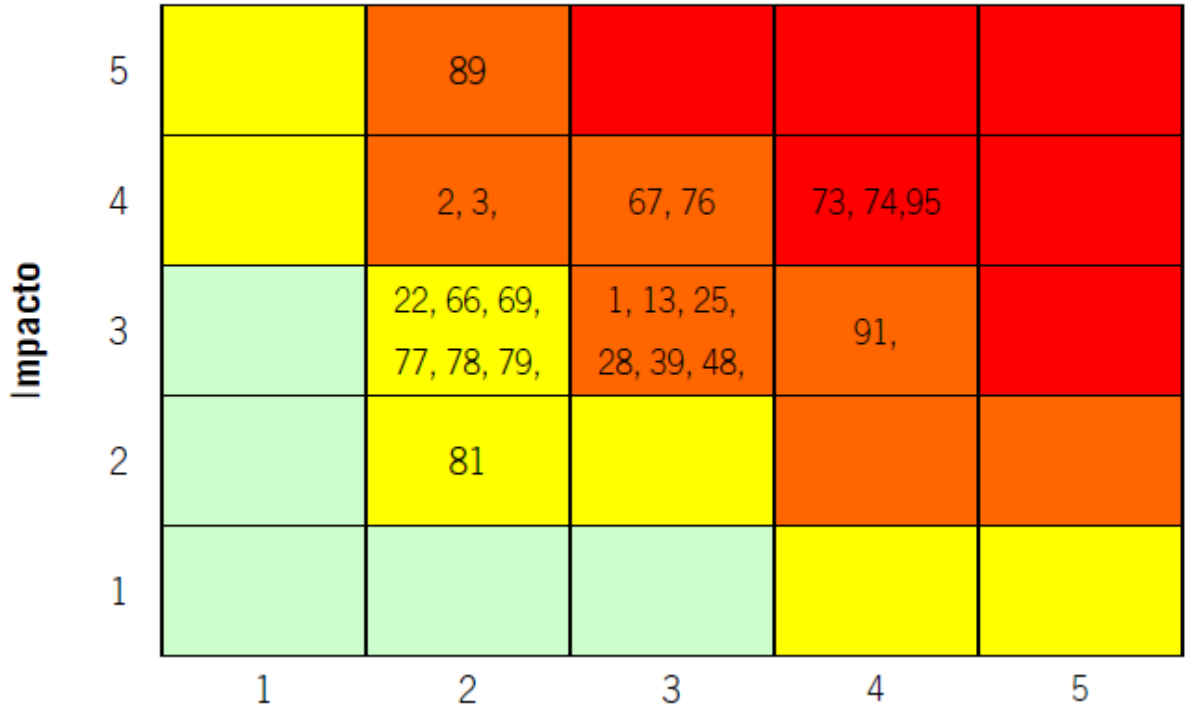
Evaluación de riesgos

Mapas térmicos riesgos absolutos

Infraestructura



Inserción tecnológica (Gestión)



Identificación de Controles

Id	Descripción del riesgo	Controles
1	Adquisición de soluciones automatizadas que no satisfagan las necesidades de la institución.	Se realiza un diagnóstico sobre las necesidades y factibilidad de adquirir la solución. Se le da participación del usuario para validar las necesidades.
2	Desarrollar productos que no cumplen con las especificaciones.	Pruebas de productos basadas en casos de uso. Aprobación de fases de análisis y diseño para comprobar el alcance.

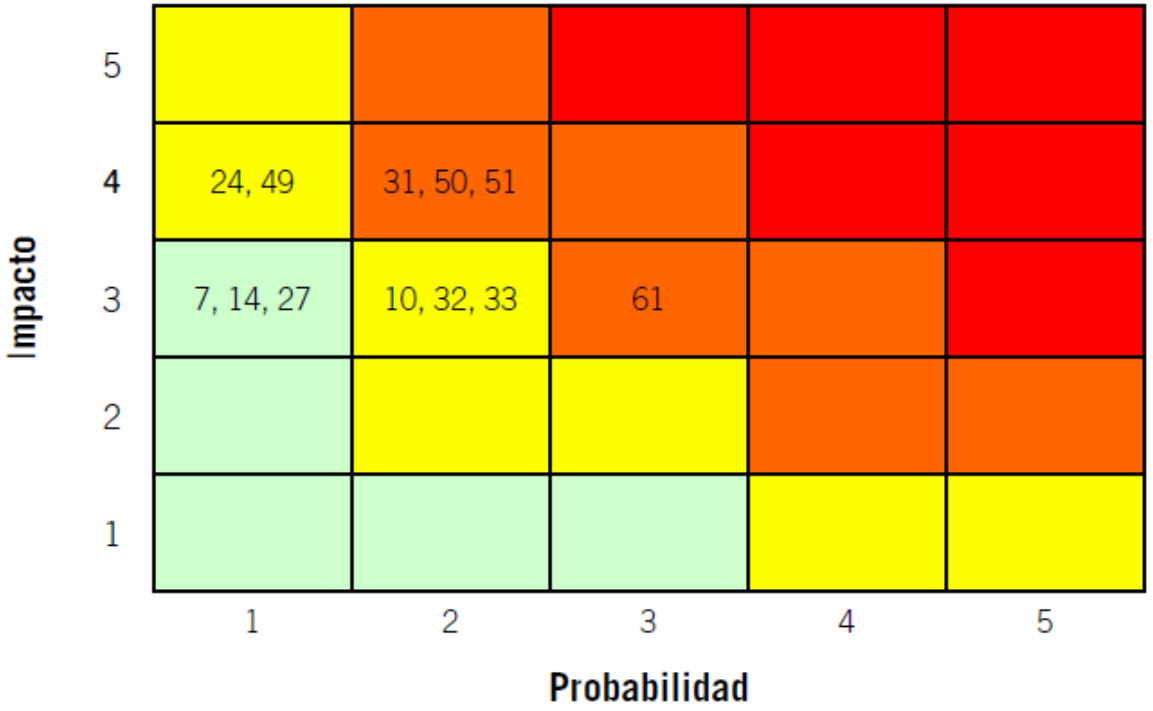
Evaluación de riesgos controlados

Id	Riesgo	P	I	S
1	Adquisición de soluciones automatizadas que no satisfagan las necesidades de la institución.	1	3	3
2	Desarrollar productos que no cumplen con las especificaciones.	1	4	4
3	Desarrollar productos basados en requerimientos incorrectos.	1	4	4
4	Versiones de software desactualizadas.	2	4	8
5	Adquirir software sin programas fuentes.	1	4	4
6	Adquirir software que no tiene representación en el país.	1	4	4
7	Equipo dañado no puede ser reparado.	1	3	3
8	Red inalámbrica insegura.	2	3	6

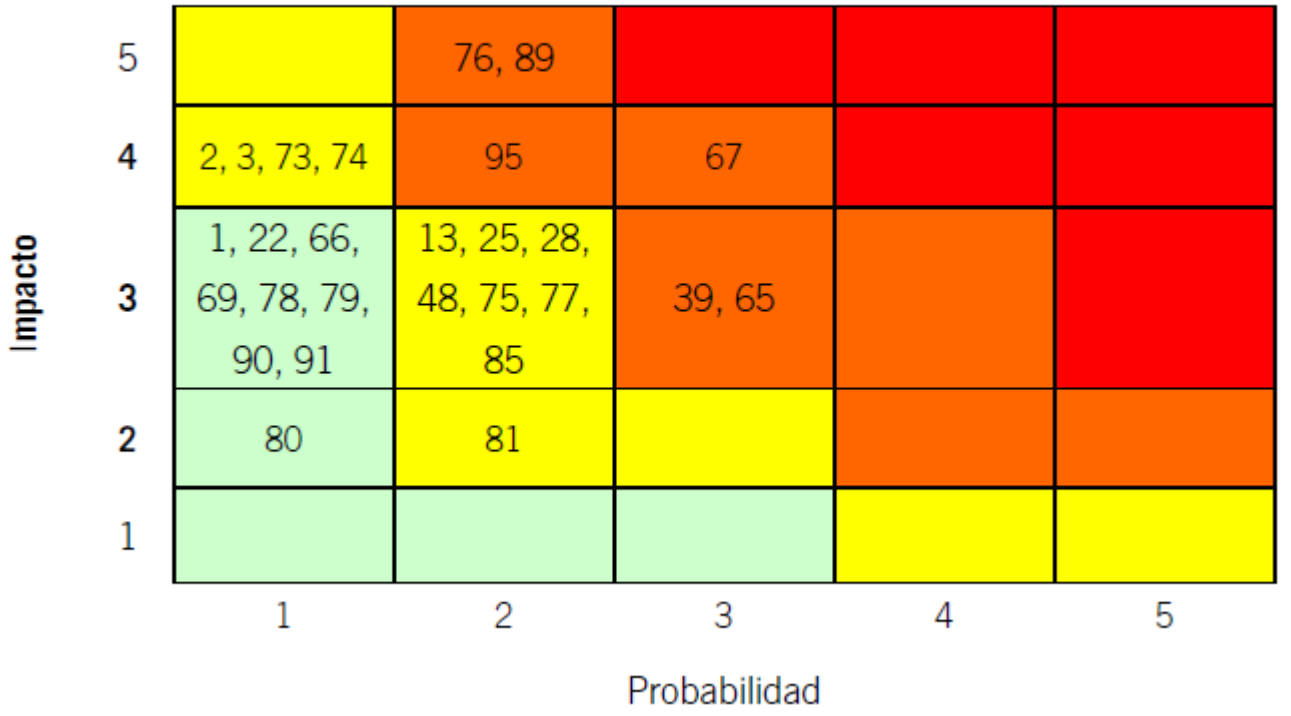
Evaluación de riesgos controlados

Mapas térmicos riesgos controlados

Infraestructura

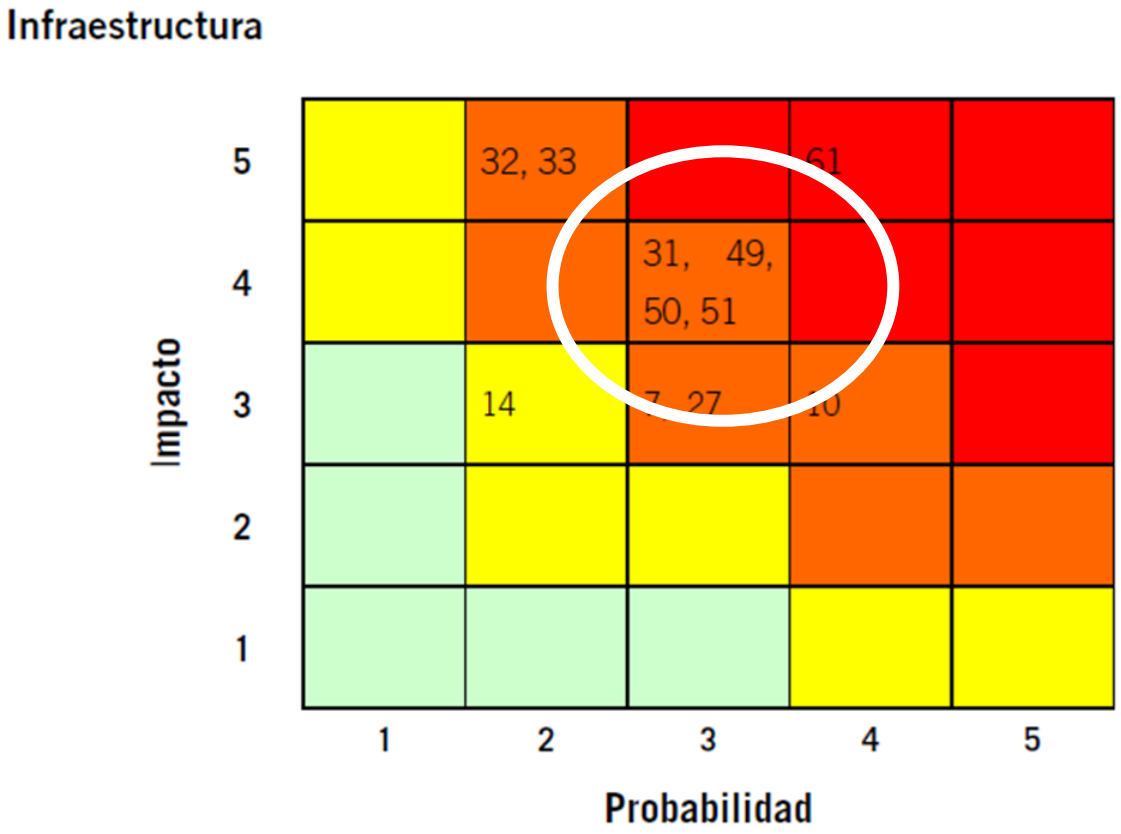


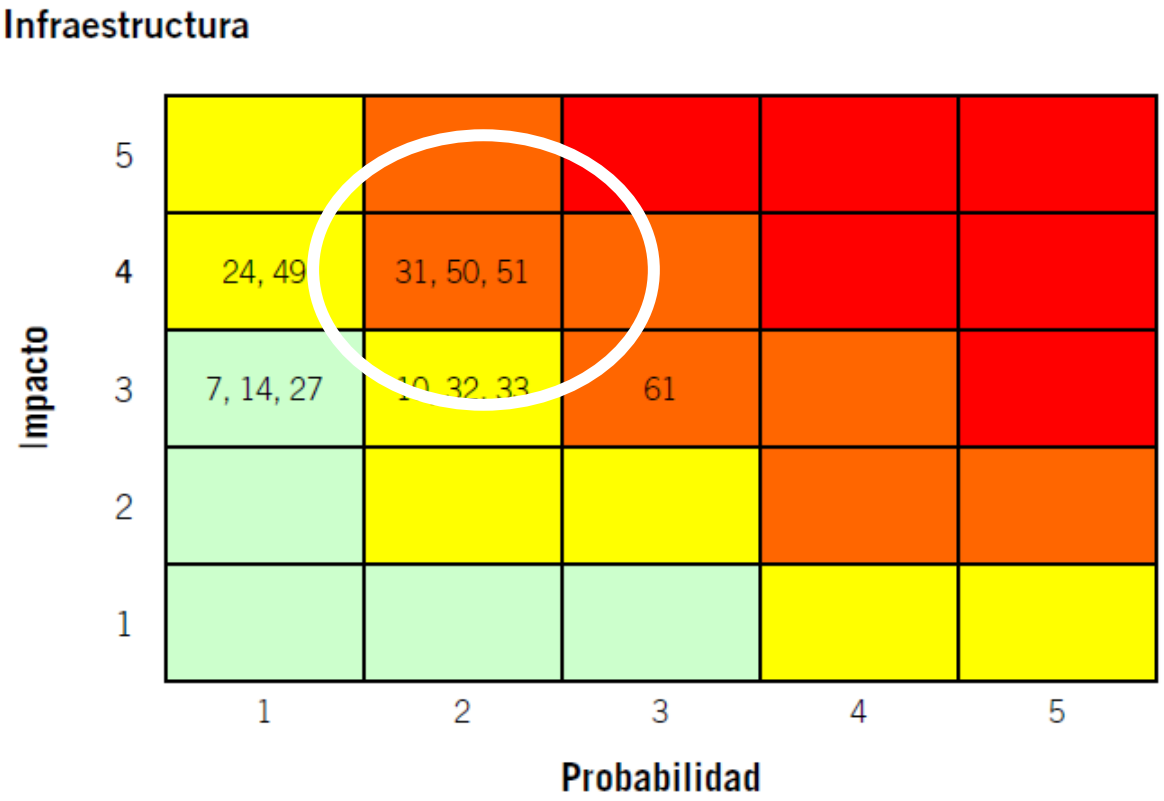
Inserción tecnológica



Criterios para incluir en la selección de auditorias

Comparación de Mapas térmicos





Criterios para incluir en la selección de auditorias

- Controles que representen Inversiones
- Controles que no hayan disminuido el riesgo.
- Controles que hayan disminuido mínimamente los riesgos.
- Controles que representen gasto elevado.
- Controles con incluyen asesorías.
- Otros criterios