

## ANEXO

### MATRIZ DE RIESGOS

La presente Matriz de Riesgos tiene como objetivo identificar, analizar y gestionar los riesgos asociados a la ejecución del proyecto: "Prestar servicios tecnológicos especializados para el fortalecimiento de la infraestructura tecnológica del ColCERT, mediante la actualización de licenciamiento especializado en seguridad digital, así como la prestación de servicios técnicos asociados a dicho licenciamiento, incluyendo el monitoreo, detección y respuesta ante incidentes de seguridad digital (MDR), y el soporte y mantenimiento del sistema de videowall, de conformidad con las condiciones y alcances definidos en el Anexo Técnico, en el marco de la ejecución del Componente 1 del contrato interadministrativo suscrito entre la Corporación Agencia Nacional de Gobierno Digital – AND y el Fondo Único de Tecnologías de la Información y las Comunicaciones – FUTIC" considerando su naturaleza, alcance y contexto particular.

Los riesgos aquí descritos constituyen un referente general, por lo cual deberán ser ajustados, complementados o redefinidos por el equipo responsable, de acuerdo con las características específicas del Proyecto al cual se aplique la matriz.

La valoración de los riesgos se realizará conforme a la matriz de probabilidad e impacto definida por la gerencia del proyecto, y podrá actualizarse durante el ciclo de vida del Proyecto según se identifiquen nuevos riesgos o cambios en el contexto.

Los riesgos se definen como la probabilidad de que ocurra un evento positivo (oportunidad) o negativo (amenaza) que pueda afectar la ejecución y cumplimiento de lo pactado en el proyecto.

La función de la gestión de riesgos es identificar, estudiar y tratar las causas de riesgo antes de que se materialice la situación que genera el riesgo.

Cualquier práctica ágil integra la gestión de riesgos, ya que los ciclos iterativos cortos minimizan cualquier impacto imprevisto en el desarrollo del proyecto. El SBOK® (Scrum Body of Knowledge, por ScrumStudy®) indica cómo Scrum, a través de su propio funcionamiento minimiza los riesgos teniendo en cuenta lo siguiente:

- **La flexibilidad reduce los riesgos relacionados con el negocio:** Ya que, en cualquier momento se pueden introducir o eliminar requisitos (requerimientos), y el nivel directivo/cliente está involucrado desde la perspectiva del negocio.

- **El Feedback periódico reduce los riesgos relativos a expectativas:** Así, frecuentemente, se puede responder a la pregunta “¿Hay algún requisito que ha sido mal entendido?”
- **La propiedad colectiva del proyecto** por parte del equipo de desarrollo y su responsabilidad colectiva respecto al éxito o fracaso del proyecto, **reduce los riesgos de estimaciones:** al crear un mayor compromiso del equipo en alcanzar sus objetivos.
- **El principio de transparencia reduce la no detección de riesgos:** El artefacto clave es el tablero de Scrum o Kanban, en el que se indican las actividades a realizar por el equipo y que todos pueden consultar, para el caso del proyecto el inventario de actividades del backlog (cronograma). En él se incluyen los impedimentos (problemas o riesgos de ejecución), que el equipo va encontrando y que pueden afectar al resultado del sprint. Es el rol de Scrum Máster quien tiene que gestionarlos para evitar que impacten en la eficiencia del equipo, este rol es asumido por el Gerente del Proyecto de la AND.
- **La entrega iterativa reduce los riesgos de inversión:** De forma que al ir disponiendo de productos “usables” muy pronto, se detectan antes las posibles incongruencias con el mercado y así ser capaces de reorientar el producto y la inversión asociada.

Por otro lado, PMI en la guía ACP-BOK (Agile Certified Practitioner – Body Of Knowledge) indica que los entornos de alta variabilidad, por definición, incurren en mayores incertidumbres y riesgo. Para hacer frente a esto, los proyectos gestionados mediante enfoques adaptativos hacen uso de frecuentes revisiones de los productos de trabajo incrementales y de los equipos de proyecto multidisciplinarios, a fin de acelerar el intercambio de conocimientos y garantizar que el riesgo sea comprendido y controlado.

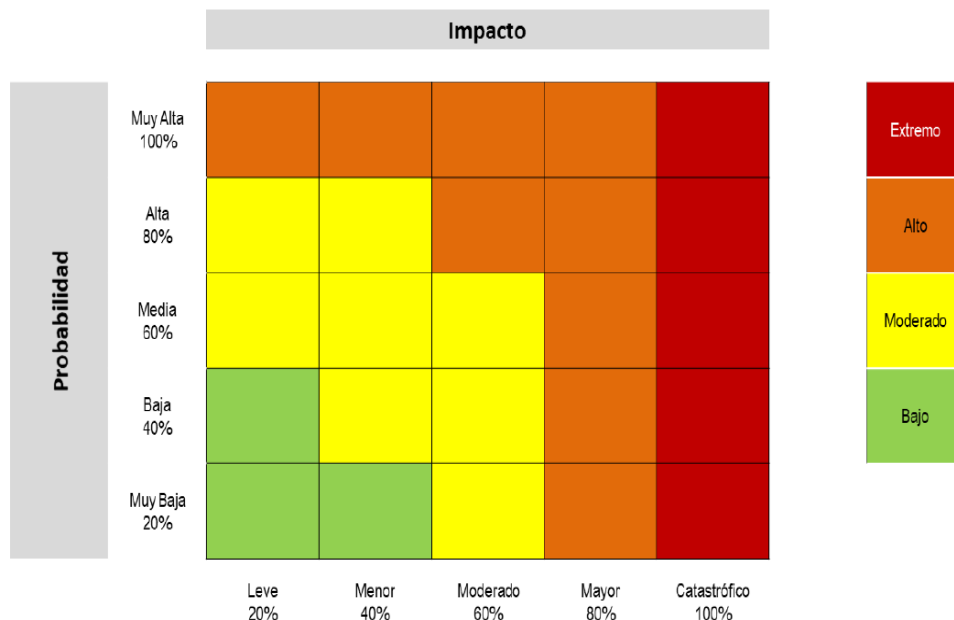
El riesgo se considera a la hora de seleccionar el contenido de cada iteración, y los riesgos también serán identificados, analizados y gestionados durante cada iteración en las ceremonias de la práctica. Además, los requisitos se mantienen como un documento vivo que se actualiza regularmente, y las prioridades del trabajo se pueden cambiar conforme avanza el proyecto, basándose en una mejor comprensión de la exposición al riesgo actual.

De lo expuesto en el punto anterior, se puede pensar que no hay que realizar ninguna tarea especial para gestionar riesgos. Ni crear perfiles específicos, como ocurre en la práctica predictiva de gestión de proyectos. Pero la realidad y la práctica nos dicen que no es suficiente. De hecho, de acuerdo con Martin Tomanek and Jan Juricek (Department of Systems Analysis, University of Economics, Prague, Czech Republic), denominado Project Risk Management model basado en PRINCE2® y el marco de la práctica Scrum, resalta los siguientes tópicos:

- Inexistencia de formalidad en la gestión de riesgos en metodologías ágiles.

- Controlar los riesgos en proyectos de suministro de Hardware o Software es considerado como una de las mayores contribuciones al éxito del proyecto.
- Muchos de los problemas –relativos a la gestión de riesgos–, pueden ser solucionados aplicando y alineando las técnicas y buenas prácticas, aplicadas a riesgos y usadas en la gestión de proyectos que podríamos denominar “tradicional”.
- La falta de una adecuada gestión de riesgos es uno de los principales factores por los que un proyecto fracasa.

La valoración de riesgos generales para proyectos y gestión de servicios de tecnología (Entre otros, desarrollos, soporte y mantenimiento de aplicativos, asistencia técnica en infraestructura, provision de Hardware, y proyectos asociados a tecnología, etc.) de la Subdirección de Desarrollo y Servicios Ciudadanos Digitales se realizó conforme al siguiente matriz de calor:



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP, 2026

**Figura1 Matriz de Calor**

El equipo responsable de la ejecución del proyecto puede usar un registro de riesgos y la lista de impedimentos, o lo que considere oportuno, el primer caso para riesgos de entorno de los proyectos y gestión de servicios y el segundo para control de riesgos de ejecución.

Los riesgos pueden poner en peligro la consecución de los objetivos de los proyectos y la gestión de servicios de software o hardware, pero no son lo peor que nos podría ocurrir, ya que son los problemas –impedimentos- los que no se pueden prevenir y que, al no haber sido identificados previamente, su impacto en el equipo en lo relativo a la aparición de crisis es mayor. **El hecho de identificar un riesgo reduce su impacto y/o probabilidad, si se actúa de forma proactiva.**

En la siguiente matriz elaborada con base en la “guía para la administración del riesgo y el diseño de controles en entidades públicas” del Departamento Administrativo de la Función Pública, se resumen los riesgos generales de entorno preliminares para proyectos y gestión de servicios de tecnología.

La presente matriz deberá ser revisada y actualizada por la gerencia/Supervisión del proyecto, de acuerdo con la evolución del Proyecto, y hará parte integral de la gestión de riesgos definida para su ejecución.

**Tabla 1: Riesgos Precontractuales**

| No | Clasificación | Riesgo                                                   | Causa                                          | Consecuencia                          | Responsable  | Probabilidad | Impacto | Nivel | Controles / Tratamiento                                                       | Evaluación |
|----|---------------|----------------------------------------------------------|------------------------------------------------|---------------------------------------|--------------|--------------|---------|-------|-------------------------------------------------------------------------------|------------|
| 1  | Operativo     | Definición incompleta del alcance contractual            | Levantamiento o insuficiente de requerimientos | Ambigüedad en ejecución y sobrecostos | AND          | Media        | Alto    | Alto  | Mesas técnicas previas, validación interáreas, revisión jurídica y financiera | ALTO       |
| 2  | Operativo     | Desalineación entre anexos técnicos y objeto contractual | Falta de articulación técnica-jurídica         | Observaciones o nulidades             | AND          | Media        | Alto    | Alto  | Comité de revisión integral de documentos                                     | ALTO       |
| 3  | Técnico       | Subestimación del esfuerzo operativo (MDR y licencias)   | Supuestos incorrectos                          | Insuficiencia presupuestal o retrasos | AND / Aliado | Media        | Medio   | Medio | Análisis de mercado y revisión histórica                                      | MEDIO      |
| 4  | Gobernanza    | Definición inadecuada de roles y responsabilidad         | Falta de claridad en modelo de gobierno        | Conflictos operativos                 | AND          | Media        | Medio   | Medio | Matriz RACI y modelo de gobierno del proyecto                                 | MEDIO      |
| 5  | Selección     | Imprecisiones en documentos de selección                 | Redacción ambigua                              | Dificultad en evaluación              | AND          | Baja         | Medio   | Bajo  | Revisión cruzada técnica y jurídica                                           | BAJO       |

**Tabla 2: Riesgos contractuales y de Ejecución:**

| No | Clasificación                 | Riesgo                                           | Causa                            | Consecuencia                       | Responsable  | Probabilidad | Impacto | Nivel | Controles / Tratamiento                                 | Evaluación |
|----|-------------------------------|--------------------------------------------------|----------------------------------|------------------------------------|--------------|--------------|---------|-------|---------------------------------------------------------|------------|
| 6  | Contractual                   | Condiciones técnicas o financieras insuficientes | Planeación inadecuada            | Incumplimiento parcial             | AND / Aliado | Media        | Alto    | Alto  | Seguimiento contractual y control de alcance            | ALTO       |
| 7  | Ejecución                     | Retrasos en inicio del contrato                  | Incumplimiento de requisitos     | Afectación cronograma              | Aliado       | Media        | Alto    | Alto  | Verificación previa requisitos de ejecución             | ALTO       |
| 8  | Licenciamiento                | Retraso o no renovación de licencias             | Fallas administrativas           | Interrupción servicio MDR          | Aliado       | Alta         | Alto    | Alto  | Alertas de vencimiento y contratos con fabricantes      | ALTO       |
| 9  | Tecnológico                   | Fallas en integración de herramientas (SOC, MDR, | Incompatibilidad técnica         | Interrupciones operativas          | Aliado       | Media        | Alto    | Alto  | Pruebas piloto y soporte fabricante                     | ALTO       |
| 10 | Seguridad de la Información   | Fuga o vulneración de datos                      | Fallas en controles de acceso    | Sanciones legales y reputacionales | Aliado       | Media        | Alto    | Alto  | MFA, cifrado, auditorías y cumplimiento Ley 1581/2012   | ALTO       |
| 11 | Operativo                     | Saturación de alertas sin capacidad de respuesta | Alta volumetría de eventos       | Incidentes no gestionados          | Aliado       | Alta         | Alto    | Alto  | Automatización, priorización y ampliación capacidad SOC | ALTO       |
| 12 | Infraestructura               | Indisponibilidad de infraestructura crítica      | Fallas técnicas                  | Interrupción servicio              | Aliado       | Media        | Alto    | Alto  | Plan de contingencia y redundancia                      | ALTO       |
| 13 | Talento Humano                | Insuficiencia o falta de idoneidad del equipo    | Alta rotación o mala selección   | Deficiencia en servicio            | Aliado       | Media        | Medio   | Medio | Exigencia perfiles mínimos y reemplazo inmediato        | MEDIO      |
| 14 | Gestión del Proyecto          | Retrasos por complejidad técnica                 | Dependencias no previstas        | Incumplimiento cronograma          | AND / Aliado | Media        | Medio   | Medio | Metodología ágil y entregables incrementales            | MEDIO      |
| 15 | Transferencia de Conocimiento | Falta de apropiación por parte del cliente       | Capacitación insuficiente        | Dependencia del proveedor          | Aliado       | Media        | Alto    | Alto  | Plan formal de capacitación y documentación             | ALTO       |
| 16 | Expectativa de Servicio       | Diferencias en percepción del servicio           | Expectativas no alineadas        | Reclamos contractuales             | AND / Aliado | Media        | Medio   | Medio | Socialización de alcance y SLA definidos                | MEDIO      |
| 17 | Fuerza Mayor                  | Paros, disturbios o eventos externos             | Factores externos                | Retrasos ejecución                 | AND / Aliado | Baja         | Alto    | Medio | Cláusulas de fuerza mayor y seguros                     | MEDIO      |
| 18 | Normativo                     | Cambios regulatorios                             | Nueva normativa TIC              | Ajustes contractuales              | Externo      | Baja         | Medio   | Bajo  | Seguimiento normativo                                   | BAJO       |
| 19 | Legal                         | Incumplimiento en protección de datos            | Fallas en cumplimiento normativo | Sanciones                          | Aliado       | Media        | Alto    | Alto  | Validación legal y cumplimiento normativo               | ALTO       |
| 20 | Calidad del Servicio          | Incumplimiento en SLA o calidad                  | Deficiencia operativa            | Multas o sanciones                 | Aliado       | Media        | Alto    | Alto  | Garantía de cumplimiento y penalidades                  | ALTO       |
| 21 | Informes y Reportes           | Retraso en entrega de informes                   | Falta de seguimiento             | Incumplimiento contractual         | Aliado       | Media        | Medio   | Medio | Cronograma y automatización de reportes                 | MEDIO      |
| 22 | Plan de Contingencia          | Fallo en activación ante incidente mayor         | Falta de pruebas                 | Impacto crítico en operación       | Aliado       | Alta         | Alto    | Alto  | Simulacros periódicos y pruebas de continuidad          | ALTO       |
| 23 | Judicial                      | Procesos legales del aliado                      | Litigios en curso                | Afectación financiera              | Aliado       | Media        | Alto    | Alto  | Declaración de procesos y monitoreo financiero          | ALTO       |
| 24 | Laboral                       | Reclamos laborales del personal del              | Incumplimiento laboral           | Responsabilidad solidaria          | Aliado       | Media        | Medio   | Medio | Garantía de pago de prestaciones                        | MEDIO      |
| 25 | Cierre Contractual            | Retrasos en liquidación                          | Falta de acuerdo entre partes    | Demora administrativa              | AND / Aliado | Baja         | Medio   | Bajo  | Actas parciales de aceptación                           | BAJO       |



**JULIO ERNESTO ECHAVARRIA POVEDA**  
**Subdirector de desarrollo y servicios ciudadanos digitales**  
**AGENCIA NACIONAL DIGITAL**

**Elaboró:** David Leonardo Medina. – Contratista – Subdirección de Desarrollo Y SCD



**Revisó componente Jurídico:** Christian Santiago Guzmán López. Contratista Subdirección Jurídica.

