**UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN**

**FACULTAD DE INGENIERÍA**

**ESCUELA DE FORMACIÓN PROFESIONAL DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN**

****

**SISTEMA DE IMPLEMENTACIÓN DE TI GOBIERNO REGIONAL DE PASCO**

**(Parte faltante: N° 4)**

**PRESENTADO POR:**

TORRES LUCAS, Luis

**DOCENTE:**

Ing. VICENTE GUERRA, Nilton Luis

ÍNDICE

[4. Análisis y Tratamiento de Riesgos 3](#_Toc203393537)

[1. Riesgos Internos 3](#_Toc203393538)

[Recursos Humanos 3](#_Toc203393539)

[Procesos 3](#_Toc203393540)

[Tecnología 3](#_Toc203393541)

[Operativos 4](#_Toc203393542)

[2. Riesgos Externos 4](#_Toc203393543)

[Factores Legales y Normativos 4](#_Toc203393544)

[Factores Ambientales y Naturales 4](#_Toc203393545)

[Factores Políticos y Sociales 4](#_Toc203393546)

[Relaciones con Proveedores y Terceros 4](#_Toc203393547)

# 4. Análisis y Tratamiento de Riesgos

## 1. Riesgos Internos

### Recursos Humanos

* **Falta de personal especializado en TI:**
  + **Análisis:** Puede impactar negativamente en la implementación y mantenimiento del sistema de TI.
  + **Tratamiento:** Capacitación continua, contratación de personal cualificado, colaboración con consultores externos.
* **Alta rotación del personal:**
  + **Análisis:** Podría afectar la continuidad y estabilidad del proyecto.
  + **Tratamiento:** Mejora de condiciones laborales, programas de retención de talento.
* **Resistencia al cambio:**
  + **Análisis:** Obstáculo significativo en la adopción del nuevo sistema.
  + **Tratamiento:** Plan de comunicación y gestión del cambio, involucramiento temprano de los usuarios clave.

### Procesos

* **Deficiencias en gestión de cambios tecnológicos:**
  + **Análisis:** Riesgo de interrupciones y errores durante las actualizaciones.
  + **Tratamiento:** Implementación de procesos robustos de gestión de cambios, revisiones periódicas.
* **Falta de políticas claras de actualización y mantenimiento:**
  + **Análisis:** Puede llevar a la obsolescencia y vulnerabilidades de seguridad.
  + **Tratamiento:** Desarrollo e implementación de políticas claras de mantenimiento preventivo y correctivo.
* **Falta de integración entre procesos administrativos y tecnológicos:**
  + **Análisis:** Puede generar ineficiencias operativas y errores de datos.
  + **Tratamiento:** Desarrollo de interfaces y protocolos de comunicación entre departamentos.

### Tecnología

* **Infraestructura tecnológica obsoleta:**
  + **Análisis:** Limitaciones en capacidad y disponibilidad.
  + **Tratamiento:** Plan de actualización de infraestructura, evaluación de nuevas tecnologías.
* **Problemas de compatibilidad entre sistemas:**
  + **Análisis:** Riesgo de integración y funcionamiento subóptimo.
  + **Tratamiento:** Pruebas exhaustivas de compatibilidad, desarrollo de interfaces estándar.
* **Vulnerabilidades en ciberseguridad:**
  + **Análisis:** Exposición a amenazas y ataques.
  + **Tratamiento:** Implementación de medidas de seguridad robustas, auditorías periódicas.

### Operativos

* **Errores en configuración de sistemas o migración de datos:**
  + **Análisis:** Puede resultar en pérdida de datos o interrupción de servicios.
  + **Tratamiento:** Pruebas exhaustivas, backup y planes de contingencia.
* **Fallas en la comunicación entre áreas técnicas y usuarias:**
  + **Análisis:** Riesgo de malentendidos y expectativas no cumplidas.
  + **Tratamiento:** Mejora de la comunicación interna, protocolos de reporte y seguimiento.
* **Uso inadecuado de herramientas tecnológicas:**
  + **Análisis:** Impacto en eficiencia y seguridad.
  + **Tratamiento:** Capacitación continua, guías de uso y mejores prácticas.

## 2. Riesgos Externos

### Factores Legales y Normativos

* **Cambios en normativa de adquisiciones y contrataciones:**
  + **Análisis:** Alteración de presupuestos y tiempos de entrega.
  + **Tratamiento:** Monitoreo constante de cambios regulatorios, ajuste de contratos.

### Factores Ambientales y Naturales

* **Eventos naturales (sismos, inundaciones, fallas eléctricas):**
  + **Análisis:** Riesgo de daño físico a la infraestructura.
  + **Tratamiento:** Planes de contingencia, aseguramiento de infraestructura resistente.

### Factores Políticos y Sociales

* **Cambios en la administración regional:**
  + **Análisis:** Cambios de prioridades y financiamiento.
  + **Tratamiento:** Flexibilidad en la planificación, comunicación proactiva.

### Relaciones con Proveedores y Terceros

* **Incumplimiento de cronogramas por parte de contratistas:**
  + **Análisis:** Retrasos en entregas y puesta en marcha.
  + **Tratamiento:** Supervisión continua, contratos con cláusulas de penalización.

|  |  |  |  |
| --- | --- | --- | --- |
| Categoría | Riesgo | Análisis | Tratamiento |
| Recursos Humanos (Internos) | Falta de personal especializado en TI | Impacta negativamente en la implementación y mantenimiento del sistema. | Capacitación continua, contratación de personal cualificado, consultores externos. |
|  | Alta rotación del personal | Afecta la continuidad y estabilidad del proyecto. | Mejora de condiciones laborales, programas de retención de talento. |
|  | Resistencia al cambio | Obstáculo en la adopción del nuevo sistema. | Plan de comunicación, gestión del cambio, involucramiento temprano de usuarios clave. |
| Procesos (Internos) | Deficiencias en gestión de cambios tecnológicos | Riesgo de interrupciones y errores en actualizaciones. | Procesos robustos de gestión de cambios, revisiones periódicas. |
|  | Falta de políticas de actualización y mantenimiento | Riesgo de obsolescencia y vulnerabilidades. | Desarrollo e implementación de políticas de mantenimiento preventivo y correctivo. |
|  | Falta de integración entre procesos | Ineficiencias operativas y errores de datos. | Interfaces y protocolos de comunicación entre departamentos. |
| Tecnología (Internos) | Infraestructura obsoleta | Limitaciones de capacidad y disponibilidad. | Plan de actualización tecnológica, evaluación de nuevas tecnologías. |
|  | Problemas de compatibilidad entre sistemas | Riesgo de integración deficiente. | Pruebas de compatibilidad, desarrollo de interfaces estándar. |
|  | Vulnerabilidades en ciberseguridad | Exposición a amenazas y ataques. | Seguridad robusta, auditorías periódicas. |
| Operativos (Internos) | Errores en configuración o migración | Pérdida de datos o interrupción de servicios. | Pruebas exhaustivas, respaldos, planes de contingencia. |
|  | Fallas en comunicación interna | Malentendidos y expectativas no cumplidas. | Mejora de comunicación interna, protocolos de reporte. |
|  | Uso inadecuado de herramientas tecnológicas | Afecta eficiencia y seguridad. | Capacitación continua, guías de uso y buenas prácticas. |
| Factores Legales y Normativos (Externos) | Cambios en normativas de adquisiciones | Alteración de presupuestos y cronogramas. | Monitoreo regulatorio, ajustes contractuales. |
| Factores Ambientales y Naturales (Externos) | Eventos naturales (sismos, etc.) | Riesgo de daño a la infraestructura. | Planes de contingencia, infraestructura resistente. |
| Factores Políticos y Sociales (Externos) | Cambios en administración regional | Cambios de prioridades y financiamiento. | Flexibilidad en planificación, comunicación proactiva. |
| Relación con Proveedores (Externos) | Incumplimiento de cronogramas | Retrasos en entregas y ejecución. | Supervisión continua, contratos con cláusulas de penalización. |