Anexo - NTP3

Evaluación de Riesgos en Tecnologías de Información

Introducción

Actualmente, la gestión de Tecnologías de Información y Comunicaciones (TIC) en la CGR es una de las prioridades de la agenda del Despacho de la Contralora, lo cual se evidencia en la composición de los presupuestos de tecnología, el desarrollo de proyectos, la proyección de la formación y perfil del personal de la CGR en los temas tecnológicos, así como en la elaboración de un plan estratégico, totalmente alineado con los objetivos de la institución.

En vista de la evolución de las mejores prácticas, es preciso realizar evaluaciones de riesgos constantemente, para mejorar y adecuar; si es necesario, el gobierno corporativo de las TIC, así como el marco de gestión, a los adelantos en la materia de TI.

Actualmente la CGR posee 600 computadoras de uso personal y 78 impresoras distribuidas dentro de la organización y en los grupos externos de fiscalización.

Para el almacenamiento de bases de datos se tienen dos áreas de almacenamiento en red; conectadas con fibra a servidores, con capacidades en disco de 500 GB y de 700 GB, con una ocupación total cercana al 70% de su espacio total.

Además, dispone de servidores para la ejecución de programas de seguridad, monitoreo y vigilancia. Al respecto, la disponibilidad de equipo debe ajustarse a las necesidades y prioridades que se deriven de la inserción tecnológica deseada.

Se tiene una red de área local, con sistemas tolerantes a fallas y con capacidad para enlazar a los funcionarios con sistemas de información automatizados, correo electrónico, intranet e Internet. Ahora bien, en vista de la importancia que reviste la conectividad y las nuevas tendencias móviles de la comunicación tecnológica, resulta

necesario evolucionar hacia el aprovechamiento de esas potencialidades tecnológicas en la gestión de la fiscalización.

Además, se utiliza software especializado para administrar el ancho de banda y filtrar el acceso a Internet, software de antivirus, administrador de las direcciones del protocolo de Internet (IP), la administración del firewall, los certificados privados, un administrador de proyectos, software para registro de atención de averías, el directorio activo de todos los funcionarios de la CGR, la administración de la central telefónica, el software de capacitación en línea, y la vigilancia de la seguridad de las instalaciones. Lo anterior, representa una base tecnológica que requiere ser complementada con software especializado para la fiscalización, y software colaborativo; entre otros, que permitan una fiscalización ampliamente soportada en tecnología de punta.

Finalmente, se cuenta con varios sistemas de información que soportan tanto las tareas sustantivas como las de apoyo al nivel institucional; considerándose algunos como muy críticos.

Modelo de análisis de riesgos

Contexto estratégico

La CGR es un órgano de control de la Asamblea Legislativa y tiene bajo su fiscalización 472 instituciones públicas, más Juntas de Educación, Asociaciones, y empresas privadas que administren fondos públicos, para que con base en los estudios realizados se le permita a la ciudadanía conocer, acerca de cómo sus gobernantes y funcionarios públicos están utilizando los recursos que se les asignaron. Presupuestariamente depende de un presupuesto aprobado por la Asamblea Legislativa.

Para transparentar la gestión pública se basa en su ley orgánica, la ley de control interno, en el sistema para evaluación de riesgos, en resoluciones de cumplimiento

obligatorio, y en normas técnicas sobre la gestión en tecnologías de información comunicación.

La clientela de la CGR la conforma prácticamente todo el país: ciudadanía, proveedores, instituciones, empresas, y organismos internacionales; los cuales confían en la gestión que lleva a cabo la Contraloría para garantizarle a la ciudadanía el buen manejo de la Hacienda Pública.

Además de la transparencia hacia la ciudadanía sobre la gestión de los funcionarios públicos, también es muy importante mantener el control político con el objetivo de evaluar cualquier situación que pueda afectar la estrategia.

Otro aspecto que es de importancia para la CGR es la imagen que se pueda reflejar a la ciudadanía, con el objetivo de mantener y mejorar la confianza que se tiene en la institución como garante de la Hacienda Pública.

Para dar cumplimiento al propósito de fortalecer el buen gobierno, todos los funcionarios deben tener presentes aspectos importantes de nuestra gestión, como los siguientes:

- Clasificación de las instituciones públicas con base en factores de riesgo. Esto significa que el monto del presupuesto no va a ser la única variable para determinar hacia dónde dirigir la fiscalización, sino que también interesa la calidad de la administración y sus órganos de decisión, de la auditoría interna, la contratación, la planificación, las variables financieras y otras. Es necesario que definamos un conjunto de variables y no busquemos el sistema perfecto para identificar las entidades de más riesgo y a partir de ahí definir a dónde vamos a ir y qué vamos a hacer. Esto también significa que no solo la institución esté clara hacia donde vamos, sino que los que están en el entorno también lo tengan claro, ya que lo más operativo lo

deberán asumir las auditorías internas y el mismo sistema de control de cada institución.

- Aplicación de los temas estratégicos para la fiscalización, según las particularidades de las áreas de fiscalización y los resultados de la clasificación anterior, es decir, cada área deberá dedicarse prioritariamente a algunos de los temas aquí planteados, no necesariamente a todos.
- Seguimiento de disposiciones como elemento esencial para ir midiendo el impacto de nuestra gestión.
- Elaboración de indicadores sencillos para medir los resultados propuestos en el plan de trabajo.
- Ejecución efectiva de la agenda de mejoras internas, ya que los proyectos que se definan darán el salto cualitativo que la institución requiere para tener un nivel mayor de incidencia en la gestión de las administraciones públicas.
- Recurso humano y tecnología. En relación con las personas, éstas deben ser capaces, si existe una brecha frente a las necesidades de los procesos de trabajo, esta debe cerrarse por medio de capacitación u otras acciones que les permitan desarrollar mejor sus competencias. El gerente tiene una responsabilidad importante en materia de recurso humano, tiene una responsabilidad en forma directa e inmediata en su manejo, buscando el equilibrio para lograr un desarrollo integral de la gente y hacer converger los objetivos de las personas con los de la institución. Por su parte, la tecnología es fundamental para apoyar el trabajo no solo en la simplificación sino también siendo utilizada para almacenar y proporcionar información que apoye la toma de decisiones.
- Medición del desempeño en función de resultados. Hay que darle un cambio a la evaluación del desempeño. Debe verse como una retroalimentación. Esta debe asociarse al logro de los objetivos de la unidad, más los compromisos personales. Es una evaluación asociada con resultados de proyectos tangibles.

Estos lineamientos contribuirán a la organización del trabajo y a la formulación de los planes de trabajo operativos de los próximos años de las diferentes Divisiones, Áreas y Unidades de la Contraloría General, base fundamental sobre la cual, rendiremos cuentas a la ciudadanía.

De acuerdo con sanas prácticas de gestión, todo plan institucional en la Contraloría General, debe estar directamente relacionado con los objetivos estratégicos, estrategias, factores clave de éxito y las orientaciones del Plan Estratégico Institucional 2008-2012, de ahí que el plan estratégico en tecnologías de información y comunicación (PETIC) no es una excepción, en este sentido, la gestión institucional de tecnologías de información y comunicación para el período 2008-2012, se debe realizar de acuerdo con las siguientes orientaciones estratégicas:

a. Control como medio y no como fin
b. No afectación del interés público
c. No coadministrar
d. Mayor proactividad, presencia, impacto y oportunidad
e. Enfoque preventivo
f. Énfasis en los resultados de la gestión pública
g. Fiscalización y control sobre una base costo-beneficio
h. Aplicación de procesos con base en el Manual General de la Fiscalización Integral
i. Cultura de medición continua de la gestión
j. Mejora continua que fortalezca la autocrítica constructiva

Con base a las orientaciones estratégicas se pueden observar posibles riesgos financieros, sociales, operativos, técnicos, legales, y humanos, sobre los cuales vamos a estar trabajando en el presente análisis y valoración de riesgos, siempre que estén relacionados con tecnologías de información.

Factores claves de éxito

El cumplimiento de la estrategia institucional 2008-2012 está en función de lograr la articulación de esfuerzos institucionales alrededor de los siguientes elementos:

a. Desarrollo de las competencias de los funcionarios ajustadas a los requerimientos de la CGR para enfrentar el entorno
b. Aprovechamiento de las tecnologías de información en las fiscalización y la toma de decisiones
c. Integración institucional que facilite la toma de decisiones y la consistencia de los productos de fiscalización.

Visión de la CGR

Garantizamos a la sociedad costarricense, la vigilancia efectiva de la Hacienda Pública.

Misión de la CGR

Somos el órgano constitucional, auxiliar de la Asamblea Legislativa que fiscaliza el uso de los fondos públicos para mejorar la gestión de la Hacienda Pública y contribuir al control político y ciudadano.

Valores

Los siguientes elementos constituyen la guía de actuación que debe inspirar la gestión y rectitud de los actos de los funcionarios de la Contraloría General de la República, a efecto de implementar la visión y misión institucionales:

- **Excelencia**: Búsqueda de la máxima calidad y desempeño en el trabajo diario.
- **Respeto**: Valorar los derechos y formar de pensar de los demás.

- **Justicia**: Dar a los demás lo que les corresponde de acuerdo con sus derechos y deberes.
- **Integridad**: Es realizar todas las acciones con rectitud.
- **Compromiso**: Es sentirse identificado con la Contraloría General y así dar el máximo esfuerzo.

La CGR tiene cuatro macro procesos:

a. Fiscalización Integral
b. Gobierno Corporativo
c. Gestión del Conocimiento
d. Gestión del Recurso Humano

La gestión de tecnologías de información apoya estos macro procesos con cuatro procesos:

a. Infraestructura
b. Seguridad y Control
c. Suministro de Servicios
d. Inserción Tecnológica

Sobre estos cuatro procesos se realizará una valoración de los riesgos a los cuales están expuestos, y el nivel de exposición de los mismos.

La Unidad de Tecnología de Información (UTI)

El Reglamento Orgánico de la Contraloría General de la República, emitido mediante resolución No. R-CO-34-2009 del 22 de mayo de 2009, en su Capítulo II, Sección CUARTA, artículo 26, establece con respecto a la Unidad Tecnologías de Información:

Es la unidad encargada de implementar, desarrollar y evolucionar soluciones tecnológicas y de comunicación, para apoyar y facilitar la ejecución de los procesos internos Para ello lidera el proceso de gestión de tecnologías de información y comunicación y participa del proceso de asesoría interna en materia de su competencia.

Visión de la UTI

Una Contraloría General posicionada y ampliamente digitalizada, con acceso inmediato a la información, con eficientes herramientas tecnológicas de apoyo para realizar fiscalización de la Hacienda Pública; todo con el objetivo de transparentar la gestión pública, fomentar la participación ciudadana, combatir la corrupción y apoyar el buen Gobierno.

Misión de la UTI

Somos una Unidad especializada para brindar servicios oportunos en tecnologías de información y comunicación para fortalecer la fiscalización superior, la transparencia, la participación ciudadana, y la rendición de cuentas por medio de la gestión realizada en la Contraloría General.

Objetivos de la UTI

Los siguientes son los objetivos estratégicos de la UTI:

a. Contar con una infraestructura de Tecnologías de Información y Comunicaciones (TICs) estable y adecuada a las necesidades de la Institución y del país.

b. Alinear la plataforma tecnológica hacia el logro de objetivos institucionales, integrada a procesos y actividades, y puesta al servicio de los usuarios internos y externos.

c. Desarrollar la infoestructura de soluciones y servicios definidos y priorizados en el Plan Institucional, en aras de impulsar la eficiencia, la eficacia, la transparencia, la participación ciudadana y el combatir de la corrupción.

d. Fortalecer el Gobierno Electrónico mediante transparentar la gestión pública, la simplificación de procesos, la generación de trámites electrónicos y la participación ciudadana.

e. Coordinar con el Centro de Capacitación, la capacitación de los funcionarios de la Contraloría General de la República y de otras instituciones para mejor uso y aprovechamiento de las TIC's.

f. Mantener una organización actualizada con las tendencias modernas de tecnologías de información y comunicaciones (TIC's), y con los requerimientos de información y tecnología de la institución.

Contexto de la administración de riesgos

La administración de riesgos se lleva a cabo considerando los procesos de USTI que están relacionados con las tecnologías de información y la Plan Estratégico 2008 – 2012, a efectos de establecer y fortalecimiento los controles necesarios en aquellos que así lo requieran. En la identificación de riesgos se consideran los efectos que una mala gestión pueda tener en la imagen de la CGR, las pérdidas producto de inversiones que no generen réditos, y las orientaciones estratégicas.

En los anexos 1 y 2 se presentan los riesgos relacionados con los objetivos del Plan Estratégico Institucional 2008-2012 y con los objetivos del Plan Táctico Institucional 2009-2011; riesgos que constituyen el fundamento para la valoración de riesgos a nivel operativo, y que estarán siendo aplicados y revisados en el contexto de la ejecución y seguimiento del PAO 2009 y de la formulación detallada del PAO 2010.

La evaluación de riesgos se llevará a cabo sobre los procesos de la USTI: Infraestructura, Seguridad y Control, Suministro de Servicios, e Inserción tecnológica, basados en COBIT.

Portafolio de riesgos

Marco de administración de riesgos

Es importante definir claramente el marco de trabajo que será utilizado para la gestión de los riesgos en la Unidad de Tecnologías de Información de la CGR; los objetivos son los siguientes:

a. Contar con un marco de referencia para la gestión de los riesgos; este marco de referencia debe ser conocido y comprendido por todos los miembros de la Unidad.
b. Preparar a la organización para eventos de riesgo que pueda atentar contra los servicios prestados por la UTI.
c. Orientar la gestión de la Unidad para tomar medidas que ayuden, dentro de las posibilidades de la Institución, a mantener la continuidad de las operaciones.
d. Fortalecer la imagen institucional por medio de una operación tecnológica más estable y confiable.

La estrategia para la administración de los riesgos está basada en los siguientes aspectos:

- Utilizar los sub procesos de COBIT por guía y referencia para la identificación de riesgos de gestión.
- Complementar la identificación de riesgos basándose en los procesos de la Unidad, esto para identificar riesgos operativos.
- Utilizar escalas de calificación de los riesgos (impacto, probabilidad, exposición) de acuerdo con modelos internaciones.

El alcance de este ejercicio de análisis de riesgos comprende lo siguiente:

- Actividades de gestión de la UTI las cuales están a cargo de la jefatura y de los coordinadores.
- Procesos de la UTI que incluyen las operaciones continuas y el desarrollo de proyectos
- Proyectos tecnológicos de trascendencia institucional lo cuales influyen en la imagen que se proyecta a la ciudadanía.
- Riesgos relacionados con el recurso más importante de la organización: el recurso humano.

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.

Para clasificar los riesgos se utilizarán 5 categorías asociadas con el origen del riesgo. Se utilizarán criterios de referencia específicos para cada categoría con el propósito de de facilitar la evaluación de impacto para cada riesgo.

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

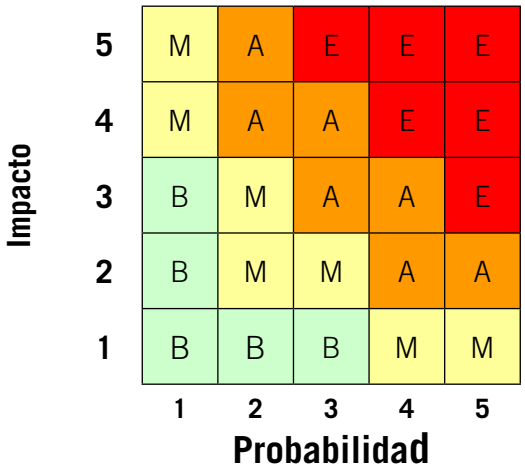
Severidad del riesgo

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 corlo en su nivel de severidad. El corlo rojo representa severidad extrema, el color naranja severidad alta, el color amarillo claro severidad moderada y el color verde claro severidad baja:



Categorías de los riesgos

Las categorías utilizadas son las siguientes:

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.

Inserción Tecnológica

Es posible que un riesgo pertenezca o está relacionado con dos o más categorías; por ejemplo, el incumplimiento de un procedimiento operativo puede dar lugar a un evento de seguridad. En estos casos el riesgo será asociado a la categoría que se considere más relevante o donde el impacto sea mayor.

Impacto de los riesgos según su categoría

Gestión

I	Significado	Criterios de calificación
5	Mayor	Evento que impedirá el logro de los objetivos institucionales.
4	Importante	El logro de objetivos institucionales se ve afectado de manera importante.
3	Significativo	Evento que representará un retraso significativo en el logro de objetivos institucionales.
2	Regular	El evento afecta levemente el logro de objetivos de la UTI y de la CGR.
1	Menor	Evento que afecta la gestión de la UTI sin llegar a impactar en el logro de los objetivos.

Operación

I	Significado	Criterios de calificación
5	Mayor	Evento que paraliza la prestación de servicios por parte de la unidad afectando a la institución de manera considerable.
4	Importante	Evento que provoca la interrupción parcial de servicios.
3	Significativo	Evento que provoca interrupciones intermitentes.
2	Regular	Evento que provoca la interrupción momentánea de los servicios de la unidad, esta interrupción es percibida por la institución. Evento que provoca una disminución en los tiempos de respuesta que experimentan los usuarios.
1	Menor	Evento que afecta sólo las operaciones de la UTI.

Infraestructura

I	Significado	Criterios de calificación
5	Mayor	Falla severa en un componente vital de la infraestructura tecnológica que impide la operación normal de la institución.
4	Importante	Falla en un componente de la infraestructura tecnológica que afecta parcialmente la prestación de servicios.
3	Significativo	Falla en un componente de la infraestructura tecnológica que afecta de manera intermitente la prestación de servicios.
2	Regular	Falla en un equipo que afecta la prestación de servicios sólo en la UTI.
1	Menor	Falla en un componente que puede ser sustituido de inmediato por mantener equipo similar en inventario. Se afecta la operación de la institución por minutos.

Seguridad

I	Significado	Criterios de calificación
5	Mayor	La seguridad es vulnerada y se desconocen sus efectos. Un ente no autorizado tiene acceso a información confidencial. Información total en la disponibilidad de información. Los datos institucionales han sido alterados.

4	Importante	Un ente no autorizado tiene acceso a información sensitiva. Interrupción de más de 1 día hábil en la disponibilidad de la información.
3	Significativo	Se reciben ataques masivos sobre la plataforma. Un funcionario de la institución tiene acceso a información a la cual no está autorizado. Interrupción de 1 día hábil en la disponibilidad de la información. Pérdida de datos que se pueden restaurar por medio de los procesos de recuperación.
2	Regular	Entes no autorizados tienen acceso a información parcial en modo consulta. Interrupción de 4 horas en la disponibilidad de la información.
1	Menor	Hay intentos de acceso a la información. Interrupción momentánea en la disponibilidad de la información. Un ente no autorizado tiene la oportunidad de observar datos que se están utilizando en la operación de la institución.

Recurso humano (Revisar objetivos)

I	Significado	Criterios de calificación
5	Mayor	Se prescinde de un funcionario importante para el logro de los objetivos. El evento imposibilita a todo el personal de la UTI para realizar sus funciones de manera indefinida. Evento que provoca que un funcionario exceda en más de un 40% el tiempo estimado para finalizar una actividad.

4	Importante	Los objetivos a lograr exceden las cargas de trabajo de los recursos asignados a la UTI. Evento que imposibilita que el personal de la UTI pueda laborar durante un día hábil. Evento que provoca que un funcionario exceda en un 40% el tiempo estimado para finalizar una actividad.
3	Significativo	No se tiene participación del patrocinador para el logro de los objetivos. Evento que imposibilita a un funcionario de la UTI para laborar durante cinco días hábiles en el lapso de un mes. Situación que provoca que un funcionario exceda en un 20% el tiempo estimado para finalizar una actividad.
2	Regular	Evento que provoca que un funcionario exceda en un 10% el tiempo estimado para finalizar una actividad. Evento que afecta, de manera temporal y no mayor de 4 horas, que los funcionarios de la UTI puedan realizar sus funciones.
1	Menor	Se asignan objetivos adicionales que afectan levemente la carga de trabajo. Evento que imposibilita a un funcionario de la UTI para laborar durante un día hábil.

Criterios para la aceptación de riesgos

Se aceptarán aquellos riesgos cuya severidad, la cual se obtiene del impacto del riesgo y su probabilidad, esté calificada como Baja y Moderada; estos valores se representan en el mapa término con los colores verde claro y amarillo claro respectivamente.

Estructura de los riesgos

Como se indicó anteriormente, la UTI apoya los macro procesos institucionales por medio de cuatro procesos; éstos son los siguientes:

Infraestructura

El proceso de infraestructura se refiere al soporte tecnológico brindado por medio de la red de comunicaciones interna, conexiones inalámbricas, acceso vía Internet a la CGR, a las unidades para almacenamiento de datos en red, a los servidores, a la plataforma de usuario final, al software en uso debidamente autorizado y soportado por la CGR, a la solución telefónica en uso, y a todos los componentes necesarios para mantener el ambiente necesario para su operación.

Seguridad y Control

En este proceso estamos hablando de las cámaras de vídeo, acceso al Centro de Cómputo y a la UTI en general, software y hardware necesario para fortalecer la seguridad y el control, monitoreo en general, administración de componentes o funcionalidades.

Suministro de Servicios

El suministro de servicios abarca acuerdos de atención de usuarios, niveles de disponibilidad de la plataforma, atención de averías, desarrollo y evolución de sistemas, operación de equipos, continuidad de los servicios, mantenimiento y reparación de equipos, conexiones de red, y evacuación de dudas.

Inserción Tecnológica

Se pretende con este proceso que todos los funcionarios utilicen la tecnología con mucho entusiasmo, que le saquen todo el provecho posible, que producto de su uso hagan aportes que faciliten el mejoramiento continuo de la plataforma, y que las inversiones en TI permitan una mejor gestión y fiscalización.

A partir de esos procesos y tomando como punto de partida los sub dominios de Cobit se realizará la identificación de los riesgos y el posterior análisis. De este modo se determinará el nivel de riesgo absoluto y controlado de cada uno de los procesos de la Unidad. Igualmente, los mapas térmicos se presentarán por cada proceso.

El beneficio de utilizar los procesos de la UTI, como elemento central en la estructura de riesgos, es que se facilita el análisis y el diseño de posteriores planes de acción ya que en cada proceso se trabajará con un sub conjunto de riesgos lo que hace el ejercicio más manejable.

Identificación de riesgos

La identificación de riesgos corresponde a la confección de una lista de los posibles eventos que pueden afectar las operaciones y los servicios ofrecidos por TI a la institución; para facilitar la posterior evaluación del riesgo en cuanto a su nivel de impacto se les asocia la categoría correspondiente:

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

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
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

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
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

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
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

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
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

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

3	Desarrollar productos basados en requerimientos incorrectos.	Ausencia de validación de requerimientos Patrocinador sin compromiso
4	Versiones de software desactualizadas.	No hay contrato de mantenimiento. Personal no está capacitado para actualizar el software. No está planificada la actualización.
5	Adquirir software sin programas fuentes.	Mala gestión en la adquisición de software Adquisición de software es imprescindible
6	Adquirir software que no tiene representación en el país.	No se tiene otra opción
7	Equipo dañado no puede ser reparado.	No hay contrato de mantenimiento. No se tienen repuestos en el país. No hay repuestos para ese equipo. No hay presupuesto para reparación.
8	Red inalámbrica insegura.	La red es vulnerable No se tiene la capacidad para configurar adecuadamente la red
9	Daño físico en los equipos de la plataforma tecnológica.	Impericia humana Alteración del sistema eléctrico Medio ambiente no apropiado Sabotaje
10	Obsolescencia de la infraestructura tecnológica.	No se tiene la expertise para actualizarla Que no se renueven los contratos de mantenimiento

11	Desarrollo de sistemas y servicios que son difíciles de utilizar para el usuario.	Mentalidad compleja para desarrollo de sistemas No se piensa en las facilidades para el cliente
12	No existe guía de usuario para el uso del sistema.	Se omitió su elaboración El sistema es muy simple de usar
13	Retrasos en los procesos de contratación administrativa.	Se apela el cartel o la adjudicación. Negligencia administrativa.
14	Se adquiere equipo no compatible con la infraestructura en uso.	Elaboración de especificaciones incorrectas Aceptación de un modelo diferente
15	Se adquiere equipo sin que existan talleres para la reparación y mantenimiento de los mismos.	No se solicita en las especificaciones de compra El proveedor es representante único en el país
16	Trabajar directamente en equipos de producción.	Se obtuvieron passwords del ambiente de producción Se autoriza realizar trabajo en este ambiente
17	Versiones de software para desarrollo y producción diferentes.	No se han actualizado El soporte en Costa Rica no es el mejor
18	No contar con la metodología y procedimientos necesarios para la administración de los cambios.	No ha sido prioritario su desarrollo.
19	Libertad en el uso de componentes tecnológicos (software libre).	No se respetan las políticas definidas No se tienen las herramientas necesarias para controlar su instalación

20	Instalación de parches sin seguir las recomendaciones del proveedor.	No se tiene control sobre los parches autorizados No se revisa la documentación del proveedor
21	Ausencia de niveles de servicio aceptados que faciliten la gestión.	No hay acuerdos de servicios de niveles.
22	Definición de niveles de servicio que sobrepasan la capacidad instalada de TI.	No se realiza el análisis de capacidades No se considera el recurso humano disponible
23	No contar con los recursos necesarios para cumplir con los niveles de servicio.	Fallas de hardware y software superan el estimado realizado Se dañan las herramientas necesarias
24	No existe contrato de mantenimiento	No se tiene presupuesto. Se encuentra en periodo de garantía. Está en trámite.
25	Debilidad en la administración de servicios de terceros que implica que éstos no cumplan satisfactoriamente los requerimientos del negocio.	No se han definido responsables por contrato. Administración de contratos no adecuada.
26	Incumplimiento de las políticas definidas por las partes.	No se gestiona con base en las políticas definidas
27	Tiempo de respuesta degradado.	Servidores ocasionalmente degradados Servidores ocasionalmente saturados Ataque a los componentes de la red Sistema consume muchos recursos (AB,CPU)

28	No hacer planeamiento de la capacidad.	La actividad no es parte del plan de gestión No se tiene la capacidad para realizarlo
29	Los recursos de la infraestructura tecnológica no son suficientes para atender las demandas de servicios.	No se planificaron las compras con base al crecimiento de la infraestructura Se da un crecimiento en recursos no planificado
30	Recuperación de software no es factible	Procedimiento para recuperación incorrecto No se cuenta con el recurso para recuperarlo
31	Suspensión de servicio de Internet	Fallas en el equipo del proveedor del servicio Se daño un componente interno Deficiencias en la administración
32	Fallas en los equipos de comunicaciones	Impericia humana Alteración del sistema eléctrico Se daño el equipo Sabotaje
33	Fallas en los servidores (computadores principales)	Impericia humana El equipo se daño Se alteró la configuración Alteración del sistema eléctrico
34	Equipo de usuario final inseguro.	Se libera el equipo de algunas políticas de seguridad cuando se trasladan a una Institución La instalación de componentes no es controlada en algunos casos

35	Ausencia de controles cruzados que comprueben la integridad de la información y el funcionamiento correcto de las aplicaciones.	No se programaron Los controles programados son débiles
36	Errores en la creación de usuarios y en la asignación de privilegios de acceso.	No se tiene el conocimiento necesario para realizar la función Se desconoce la cobertura autorizada para cada privilegio
37	Sistemas sin mecanismos de trazabilidad de transacciones (pistas de auditoría).	No se realizaron las pruebas completas sobre el sistema que se puso en producción
38	No se conocen los costos asignados a los servicios prestados por TI.	No se tiene un modelo de costos No se maneja contabilidad de costos
39	No se cuenta con un proceso de análisis para mejorar los costos que están asociados a los servicios de TI.	No se tienen los insumos necesarios No ha sido prioritario
40	El personal no cuenta con el tiempo suficiente para recibir, de manera completa, la capacitación correspondiente.	Las cargas de trabajo no están balanceadas No se tiene un plan de capacitación autorizado
41	El personal no cuenta con las actitudes y aptitudes requeridas para hacer uso de la información por medio de las soluciones automatizadas.	La utilización del sistema es compleja No se tiene cultura informatizada
42	La capacitación que se brinda a los usuarios no es efectiva para que puedan utilizar eficientemente los recursos informáticos disponibles.	El instructor no tiene facilidad para la transferencia de conocimientos La capacitación no fue práctica

43	No se cuenta con presupuesto para diseñar e implementar programas de capacitación para los usuarios.	No se presupuestaron las partidas necesarias Se recortó la partida presupuestaria
44	No contar con una respuesta oportuna y efectiva para las consultas de los usuarios de TI y a la atención de los incidentes.	Personal no capacitado. Desinterés por el usuario final. Saturación de consultas.
45	Las soluciones que se aplican, ante los incidentes reportados por los usuarios, no son efectivas.	No se aprueba la solución por parte del usuario El técnico carece del conocimiento necesario
46	Los usuarios no están informados sobre los procedimientos que se deben seguir para reportar los incidentes.	No se han divulgado los procedimientos para realizar los reportes Los usuarios han estado fuera de la institución por meses
47	No se cuenta o no se aplica el procedimiento definido para la asignación, atención y seguimiento de los incidentes.	Se presentan solicitudes de un nivel superior Se atienden incidentes no registrados en el sistema
48	No se realiza una adecuada gestión de métricas sobre los incidentes reportados y atendidos.	El sistema no genera la información necesaria para generar las métricas No se dispone del tiempo necesario
49	Se realizan cambios operativos que no se reflejan en la documentación.	No se tiene un sistema para control de cambios Se realizan cambios sin que exista la documentación formal
50	Se realizan cambios en la configuración de componentes de la infraestructura y no se reflejan en la documentación.	Los cambios se realizan bajo presión No existe un sistema para control de cambios

51	No se conoce el impacto de hacer cambios en los componentes de la configuración.	No se tiene el ambiente completo para pruebas preliminares Urgía la corrección de la configuración
52	No se aplica el procedimiento oficializado para la gestión de problemas.	Se brindan soluciones sin que se realice la gestión requerida Urge la solución del problema
53	No se documentan las soluciones aplicadas a los problemas.	No es costumbre del informático realizarlo No se aplican sanciones por la omisión
54	Hay dificultad para definir el ámbito de acción de los proveedores para la solución de problemas.	No se definieron reglas contractuales claras Los proveedores se trasladan el problema
55	Alteración o pérdida de la información registrada en base de datos o equipos.	Violación de la seguridad Programa con fallas de lógica Recuperación de la base de datos con un respaldo desactualizado Fallas en disco no perceptibles
56	Información desactualizada o incorrecta.	Registro de datos incorrecta Falla en el Webservices Desconocimiento del sistema por parte del personal usuario
57	Acceso no autorizado a la información.	Se comparte el password entre usuarios Violación de la seguridad
58	Instalaciones físicas mal diseñas que pongan en peligro la integridad del equipo de cómputo y del personal.	Estructura vieja no pensada para TI. No es importante para la administración.

59	Acceso no autorizado al centro de cómputo.	Administrador del CC lo permite Personal autorizado facilita el ingreso de otros
60	Ausencia de detectores de humo.	No se tiene el presupuesto necesario para comprarlo
61	Fallas en los equipos que mantienen el medio ambiente apropiado para la operación de TI (UPS, Aire acondicionado)	No existe contrato de mantenimiento preventivo Suministro de energía eléctrica inapropiado
62	No aplicación de las políticas para la generación de respaldos.	Falta de cintas para generar los respaldos Daño en los equipos para toma de respaldos
63	No efectuar un monitoreo constante sobre la operación de la plataforma.	Exceso de seguridad por estabilidad de la plataforma No se tienen todas las herramientas
64	Suspensión de servicios sin seguir el procedimiento establecido.	Iniciativas para suspensión de servicios sin colegiarlas La suspensión es urgente
65	No contar con un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI.	No existe sistema para evaluación del desempeño.
66	No percibir los cambios que se realizan en el entorno.	Modificaciones legales que inciden en el desarrollo Cambios tecnológicos en el entorno que afectan el desarrollo

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.	No se realizó un análisis de los indicadores que se requieren en TI
68	No contar con un programa de control interno efectivo para TI que incluya auto-evaluaciones y revisiones por parte de terceros.	No se tienen directrices No hay planificación para llevar a cabo el auto control
69	No contar con la documentación de los procesos de TI.	La documentación no fue actualizada No se tiene manual para Gobierno Corporativo
70	Uso de software no licenciado	En equipo de usuario final las políticas no estaban aplicadas Se emite una autorización temporal para pruebas
71	Exceder la cantidad de usuarios autorizados para utilizar un producto licenciado.	El software permite exceder la cantidad No se tiene control sobre los usuarios instalados
72	Facilitar los medios para la instalación de software a terceros.	Se violó la seguridad para trasladar medios de instalación de software Desconocimiento contractual
73	Contar con un plan estratégico no alineado a la estrategia institucional.	Se modifica la estrategia y no se comunica Se desarrollan sistemas que no responden a la estrategia institucional
74	Se tiene Plan Estratégico desactualizado.	No se tiene un administrador del PETIC.

75	No contar con un modelo de información del negocio que sea utilizado en la creación y actualización de los sistemas de información.	No se tienen los recursos para elaborarlo
76	Arquitectura de información desactualizada.	No se tiene un administrador de la arquitectura
77	Arquitectura de información no responde a la cadena de valor.	No se diseño la arquitectura de información con base a la cadena de valor Se construyó primero la arquitectura de información
78	Adquisición de tecnologías que no aportan valor a la organización.	Se instalan tecnologías con base a convenios Se incluyen como parte del software adquirido
79	Contar con equipo costoso que no cuenta con contratos de mantenimiento.	Se venció la garantía y no se tiene presupuesto para contratar el mantenimiento No se autoriza el gasto
80	No aplicación de los canales de comunicación establecidos para informar sobre la gestión de TI.	Problemas de gestión Facilidad de canales de comunicación no incluidos en los canales formales
81	No se tienen documentados los canales de comunicación.	Funcionan muy bien los canales informales No se han documentado los canales informales
82	No se tiene dominio sobre las herramientas en uso.	El personal no fue capacitado La transferencia tecnológica no funcionó

83	Equipo de trabajo con baja motivación, poco creativo y no comprometido con el logro de los objetivos.	Clima laboral no adecuado Se desconocen los objetivos
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.	Falta de experiencia en la administración de la calidad No existe existen directrices para administrar la calidad
85	Desarrollar productos que no cumplen con los requerimientos de calidad.	Ausencia de validación de requerimientos Omisión de pruebas de calidad Incumplimiento de plan de calidad
86	No administrar los riesgos de TI.	No existe la administración basada en riesgos No se tienen los recursos necesarios
87	Utilizar un marco de trabajo deficiente para la gestión de riesgos, y no alineado con el apetito del riesgo institucional.	No se ha brindado la capacitación necesaria. No existe la administración basada en riesgos.
88	El personal no está capacitado adecuadamente para realizar una gestión efectiva de los riesgos.	No se ha brindado la capacitación necesaria.
89	No contar con el contenido presupuestario para la ejecución de los proyectos.	Elaboración de presupuesto incorrecto. No presupuestar proyectos. Recorte presupuestario.
90	Inestabilidad en el equipo de proyecto.	Reducción de personal. Clima laboral inadecuado.

91	Desarrollo de proyectos no alineados al Plan Estratégico	Aceptar proyecto que no han sido validados contra el Plan Estratégico. Desconocimiento del Plan Estratégico. Es obligatorio desarrollarlo.
92	Los proyectos no están documentados	El personal omite la documentación La documentación existente es omisa
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.	No hay metodología oficial para la gestión de proyectos.
94	Exceder el tiempo planificado para la ejecución de los proyectos.	Planificación no adecuada Modificación en los requerimientos Reducción de recursos
95	Falta de apoyo del patrocinador del proyecto.	No se tiene interés en el proyecto No hay personal disponible

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 (se utiliza la escala de colores del mapa térmico para su representación):

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
9	Daño físico en los equipos de la plataforma tecnológica.	3	4	12
10	Obsolescencia de la infraestructura tecnológica.	3	4	12
11	Desarrollo de sistemas y servicios que son difíciles de utilizar para el usuario.	3	3	9
12	No existe guía de usuario para el uso del sistema.	3	3	9
13	Retrasos en los procesos de contratación administrativa.	3	3	9
14	Se adquiere equipo no compatible con la infraestructura en uso.	2	3	6
15	Se adquiere equipo sin que existan talleres para la reparación y mantenimiento de los mismos.	4	3	12
16	Trabajar directamente en equipos de producción.	3	4	12
17	Versiones de software para desarrollo y producción diferentes.	4	4	16
18	No contar con la metodología y procedimientos necesarios para la administración de los cambios.	3	4	12
19	Libertad en el uso de componentes tecnológicos (software libre).	3	3	9
20	Instalación de parches sin seguir las recomendaciones del proveedor.	3	3	9
21	Ausencia de niveles de servicio aceptados que faciliten la gestión.	3	3	9

22	Definición de niveles de servicio que sobrepasan la capacidad instalada de TI.	**2**	**3**	**6**
23	No contar con los recursos necesarios para cumplir con los niveles de servicio.	**2**	**3**	**6**
24	No existe contrato de mantenimiento	**3**	**4**	**12**
25	Debilidad en la administración de servicios de terceros que implica que éstos no cumplan satisfactoriamente los requerimientos del negocio.	**3**	**3**	**9**
26	Incumplimiento de las políticas definidas por las partes.	**3**	**3**	**9**
27	Tiempo de respuesta degradado.	**3**	**3**	**9**
28	No hacer planeamiento de la capacidad.	**3**	**3**	**9**
29	Los recursos de la infraestructura tecnológica no son suficientes para atender las demandas de servicios.	**3**	**4**	**12**
30	Recuperación de software no es factible	**2**	**4**	**8**
31	Suspensión de servicio de Internet	**3**	**4**	**12**
32	Fallas en los equipos de comunicaciones	**2**	**5**	**10**
33	Fallas en los servidores (computadores principales)	**2**	**5**	**10**
34	Equipo de usuario final inseguro.	**4**	**3**	**12**
35	Ausencia de controles cruzados que comprueben la integridad de la información y el funcionamiento correcto de las aplicaciones.	**2**	**4**	**8**
36	Errores en la creación de usuarios y en la asignación de privilegios de acceso.	**3**	**4**	**12**
37	Sistemas sin mecanismos de trazabilidad de transacciones (pistas de auditoría).	**3**	**4**	**12**
38	No se conocen los costos asignados a los servicios prestados por TI.	**3**	**3**	**9**
39	No se cuenta con un proceso de análisis para mejorar los costos que están asociados a los servicios de TI.	**3**	**3**	**9**
40	El personal no cuenta con el tiempo suficiente para recibir, de manera completa, la capacitación correspondiente.	**2**	**3**	**6**
41	El personal no cuenta con las actitudes y aptitudes requeridas para hacer uso de la información por medio de las soluciones automatizadas.	**2**	**3**	**6**

42	La capacitación que se brinda a los usuarios no es efectiva para que puedan utilizar eficientemente los recursos informáticos disponibles.	**2**	**2**	**4**
43	No se cuenta con presupuesto para diseñar e implementar programas de capacitación para los usuarios.	**2**	**3**	**6**
44	No contar con una respuesta oportuna y efectiva para las consultas de los usuarios de TI y a la atención de los incidentes.	**3**	**3**	**9**
45	Las soluciones que se aplican, ante los incidentes reportados por los usuarios, no son efectivas.	**2**	**4**	**8**
46	Los usuarios no están informados sobre los procedimientos que se deben seguir para reportar los incidentes.	**2**	**3**	**6**
47	No se cuenta o no se aplica el procedimiento definido para la asignación, atención y seguimiento de los incidentes.	**2**	**3**	**6**
48	No se realiza una adecuada gestión de métricas sobre los incidentes reportados y atendidos.	**3**	**3**	**9**
49	Se realizan cambios operativos que no se reflejan en la documentación.	**3**	**4**	**12**
50	Se realizan cambios en la configuración de componentes de la infraestructura y no se reflejan en la documentación.	**3**	**4**	**12**
51	No se conoce el impacto de hacer cambios en los componentes de la configuración.	**3**	**4**	**12**
52	No se aplica el procedimiento oficializado para la gestión de problemas.	**3**	**3**	**9**
53	No se documentan las soluciones aplicadas a los problemas.	**4**	**5**	**20**
54	Hay dificultad para definir el ámbito de acción de los proveedores para la solución de problemas.	**2**	**3**	**6**
55	Alteración o pérdida de la información registrada en base de datos o equipos.	**2**	**4**	**8**
56	Información desactualizada o incorrecta.	**3**	**4**	**12**
57	Acceso no autorizado a la información.	**3**	**5**	**15**
58	Instalaciones físicas mal diseñas que pongan en peligro la integridad del equipo de cómputo y del personal.	**2**	**3**	**6**
59	Acceso no autorizado al centro de cómputo.	**3**	**3**	**9**

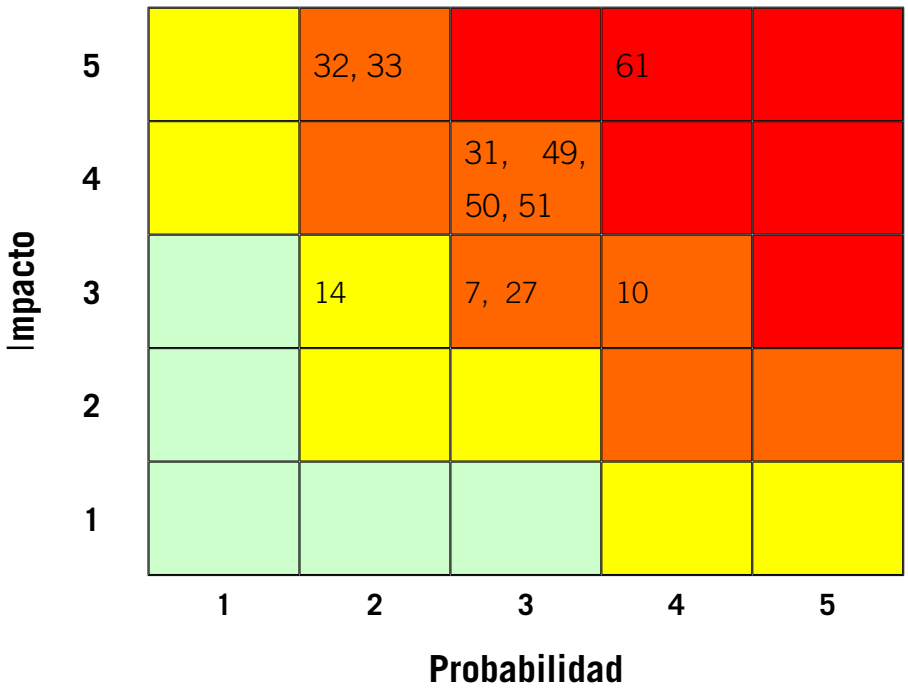
60	Ausencia de detectores de humo.	**3**	**3**	**9**
61	Fallas en los equipos que mantienen el medio ambiente apropiado para la operación de TI (UPS, Aire acondicionado)	**3**	**5**	**15**
62	No aplicación de las políticas para la generación de respaldos.	**3**	**4**	**12**
63	No efectuar un monitoreo constante sobre la operación de la plataforma.	**3**	**3**	**9**
64	Suspensión de servicios sin seguir el procedimiento establecido.	**3**	**3**	**9**
65	No contar con un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI.	**3**	**3**	**9**
66	No percibir los cambios que se realizan en el entorno.	**2**	**3**	**6**
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.	**3**	**4**	**12**
68	No contar con un programa de control interno efectivo para TI que incluya auto-evaluaciones y revisiones por parte de terceros.	**2**	**3**	**6**
69	No contar con la documentación de los procesos de TI.	**2**	**3**	**6**
70	Uso de software no licenciado	**2**	**3**	**6**
71	Exceder la cantidad de usuarios autorizados para utilizar un producto licenciado.	**2**	**3**	**6**
72	Facilitar los medios para la instalación de software a terceros.	**3**	**3**	**9**
73	Contar con un plan estratégico no alineado a la estrategia institucional.	**4**	**4**	**16**
74	Se tiene Plan Estratégico desactualizado.	**4**	**4**	**16**
75	No contar con un modelo de información del negocio que sea utilizado en la creación y actualización de los sistemas de información.	**3**	**3**	**9**
76	Arquitectura de información desactualizada.	**3**	**4**	**12**
77	Arquitectura de información no responde a la cadena de valor.	**2**	**3**	**6**
78	Adquisición de tecnologías que no aportan valor a la organización.	**2**	**3**	**6**

79	Contar con equipo costoso que no cuenta con contratos de mantenimiento.	**2**	**3**	**6**
80	No aplicación de los canales de comunicación establecidos para informar sobre la gestión de TI.	**2**	**2**	**4**
81	No se tienen documentados los canales de comunicación.	**2**	**2**	**4**
82	No se tiene dominio sobre las herramientas en uso.	**3**	**4**	**12**
83	Equipo de trabajo con baja motivación, poco creativo y no comprometido con el logro de los objetivos.	**3**	**4**	**12**
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.	**4**	**4**	**16**
85	Desarrollar productos que no cumplen con los requerimientos de calidad.	**3**	**3**	**9**
86	No administrar los riesgos de TI.	**4**	**4**	**16**
87	Utilizar un marco de trabajo deficiente para la gestión de riesgos, y no alineado con el apetito del riesgo institucional.	**4**	**4**	**16**
88	El personal no está capacitado adecuadamente para realizar una gestión efectiva de los riesgos.	**3**	**3**	**9**
89	No contar con el contenido presupuestario para la ejecución de los proyectos.	**2**	**5**	**10**
90	Inestabilidad en el equipo de proyecto.	**2**	**3**	**6**
91	Desarrollo de proyectos no alineados al Plan Estratégico	**4**	**3**	**12**
92	Los proyectos no están documentados	**4**	**4**	**16**
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.	**4**	**4**	**16**
94	Exceder el tiempo planificado para la ejecución de los proyectos.	**4**	**3**	**12**
95	Falta de apoyo del patrocinador del proyecto.	4	4	16

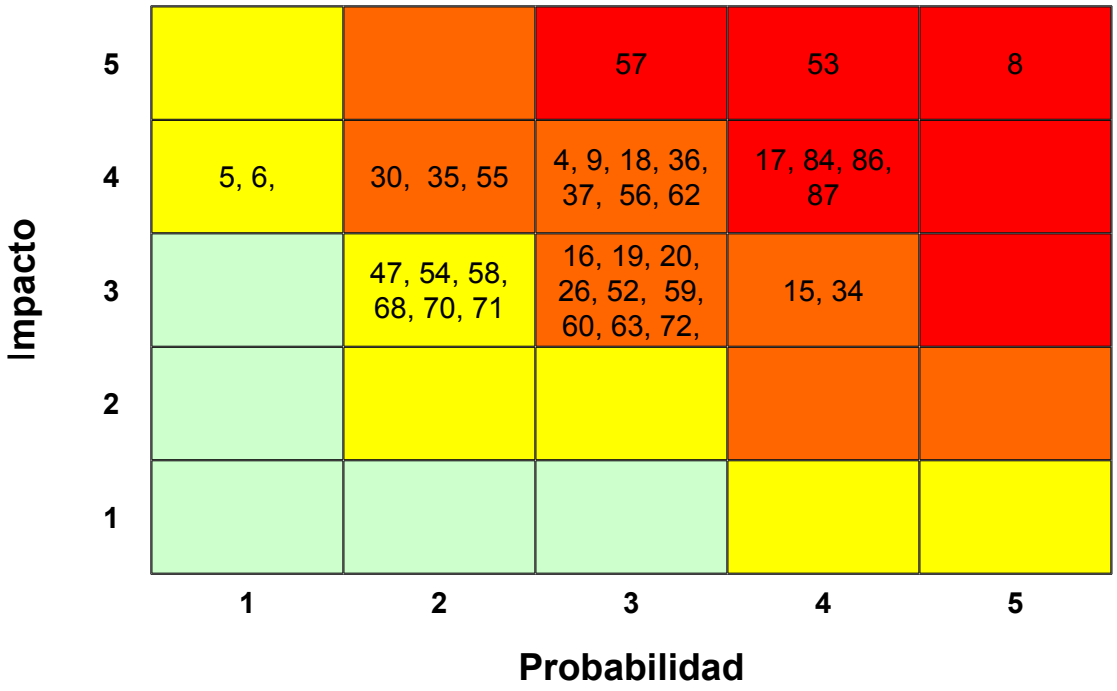
P = Probabilidad, I = Impacto, S = Severidad

Mapas térmicos riesgos absolutos

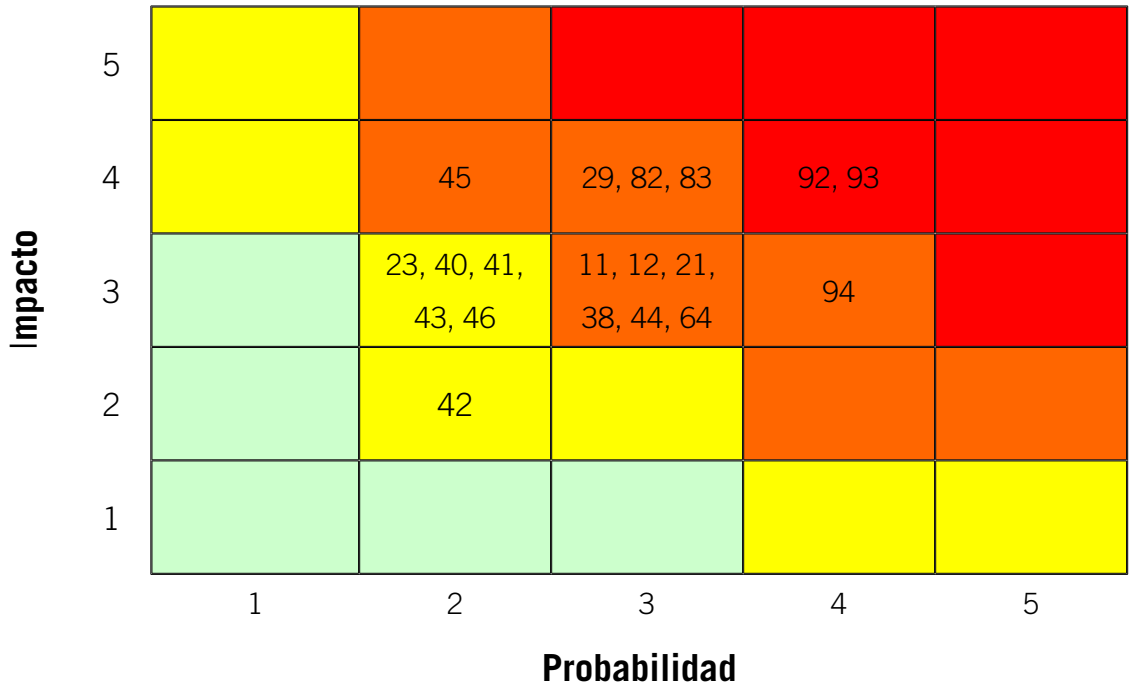
Infraestructura



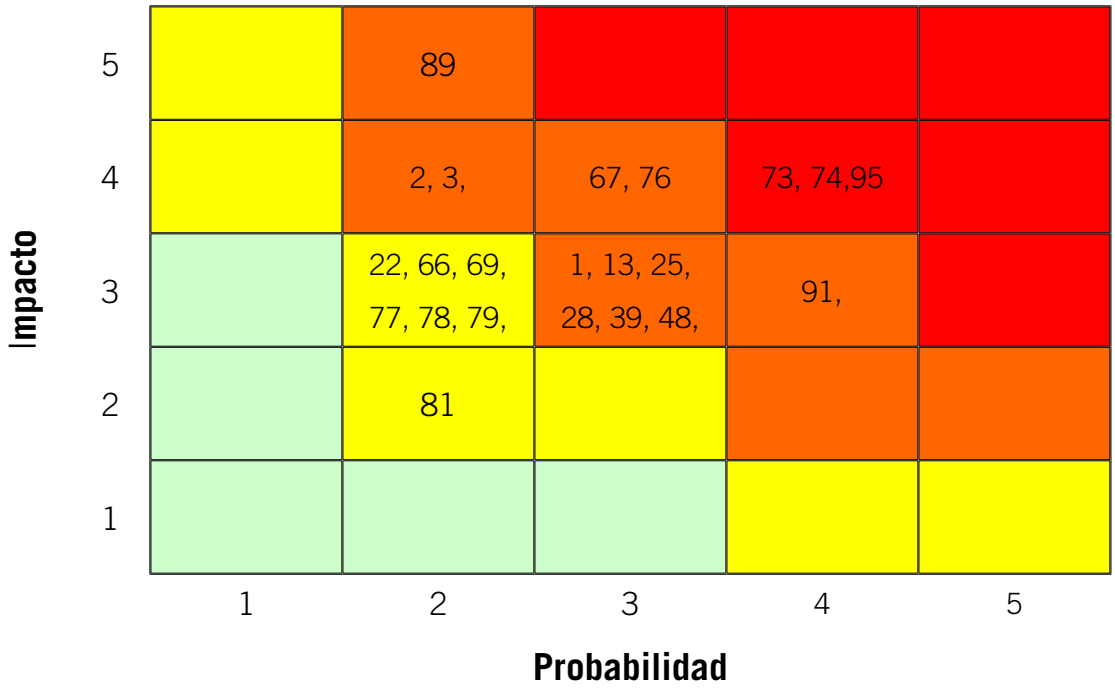
Seguridad y control



Suministro de servicios



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.

3	Desarrollar productos basados en requerimientos incorrectos.	Utilizar casos de uso para especificar los requerimientos. Validación y aprobación de los requerimientos por el patrocinador.
4	Versiones de software desactualizadas.	Por medio de los contratos de mantenimiento se planifican y aplican actualizaciones del software. Se estableció la directriz para que todos los equipos estén estandarizados en cuanto a las versiones del software.
5	Adquirir software sin programas fuentes.	Como parte de los carteles de licitación se solicitan todos los programas fuente.
6	Adquirir software que no tiene representación en el país.	La presentación del software en el país es requisito de admisibilidad de los procesos de contratación administrativa.
7	Equipo dañado no puede ser reparado.	Mantener vigentes los contratos de mantenimiento para los equipos. Contar con equipos de respaldos.
8	Red inalámbrica insegura.	Se utiliza un esquema de seguridad para restringir el acceso a la red inalámbrica. La red inalámbrica existente entre el estacionamiento y el edificio principal está totalmente separada de la red institucional.

9	Daño físico en los equipos de la plataforma tecnológica.	Se cuenta con planta de diesel y UPS. Está restringido el acceso al Centro de Cómputo. Se ha dispuesto una cámara de seguridad en la puerta. Se cuenta con sensores de temperatura y humedad.
10	Obsolescencia de la infraestructura tecnológica.	Plan de renovación y fortalecimiento de la infraestructura tecnológica. Planificación de adquisiciones con anticipación.
11	Desarrollo de sistemas y servicios que son difíciles de utilizar para el usuario.	Supervisión constante de los productos desarrollados. Revisiones de los productos por parte de los clientes.
12	No existe guía de usuario para el uso del sistema.	Se incluye información en línea para cada opción del sistema de modo que el usuario no necesite el manual. Se desarrollan tutores virtuales sobre la utilización de los sistemas.
13	Retrasos en los procesos de contratación administrativa.	Se revisan previamente los carteles para validar que estén redactados de forma clara y precisa.
14	Se adquiere equipo no compatible con la infraestructura en uso.	Revisión de los carteles. Adquisición de tecnología de arquitectura abierta.
15	Se adquiere equipo sin que existan talleres para la reparación y mantenimiento de los mismos.	Es un requisito de admisibilidad, dentro de los procedimientos de contratación administrativa, que los potenciales oferentes cuenten con el respectivo taller de servicio.

16	Trabajar directamente en equipos de producción.	Se cuenta con un servidor de desarrollo. Aplicación del procedimiento para la puesta en producción de los nuevos programas.
17	Versiones de software para desarrollo y producción diferentes.	Aplicación del procedimiento para la puesta en producción de los programas nuevos y modificados.
18	No contar con la metodología y procedimientos necesarios para la administración de los cambios.	Se han definido responsabilidades y funciones. Se cuenta con un procedimiento para aplicar los cambios en los sistemas de información.
19	Libertad en el uso de componentes tecnológicos (software libre).	Definición y aplicación de políticas institucionales sobre el uso de software autorizado y estándar para la institución. Los perfiles de usuario no tienen autorización para instalar software.
20	Instalación de parches sin seguir las recomendaciones del proveedor.	Se revisan las indicaciones de los proveedores. Los parches se aplican primero en equipo de prueba.
21	Ausencia de niveles de servicio aceptados que faciliten la gestión.	Se utiliza un software para gestionar las solicitudes de servicio pero los tiempos de respuesta esperados no están acordados.

22	Definición de niveles de servicio que sobrepasan la capacidad instalada de TI.	Análisis del PAO y portafolio de proyecto en conjunto con la Gerencia de División tomando en cuenta las cargas de trabajo y el personal actual.
23	No contar con los recursos necesarios para cumplir con los niveles de servicio.	Se cuenta con equipo renovado que presenta niveles aceptables de estabilidad.
24	No existe contrato de mantenimiento	Desarrollo periódico del Diagnóstico de Necesidades de Capacitación (DNC). Ejecución del programa de capacitación (de acuerdo con el disponible presupuestario).
25	Debilidad en la administración de servicios de terceros que implica que éstos no cumplan satisfactoriamente los requerimientos del negocio.	En el área de infraestructura se realiza un seguimiento periódico de los contratos para validar el cumplimiento de derechos adquiridos por la institución.
26	Incumplimiento de las políticas definidas por las partes.	Se analizan las cláusulas de los contratos y se giran las instrucciones del caso.
27	Tiempo de respuesta degradado.	Monitoreo de los servicios para determinar cargas de trabajo. Balanceo de cargas de trabajo (distribución de funciones entre los servidores).

28	No hacer planeamiento de la capacidad.	Antes de liberar un nuevo servicio se realizan proyecciones sobre las capacidades requeridas y disponibles. Una vez al año se realiza un ejercicio para valorar la capacidad instalada y las proyecciones de nuevos requerimientos; esto se hace como insumo para el Plan de Compras Institucional.
29	Los recursos de la infraestructura tecnológica no son suficientes para atender las demandas de servicios.	Se planifica la adquisición de tecnología para mantener la capacidad de procesamiento de información.
30	Recuperación de software no es factible	Revisión de los respaldos generados. Se cuenta con equipos que se pueden utilizar, ante contingencias, para reestablecer los servicios.
31	Suspensión de servicio de Internet	Se cuenta con una red moderna que da estabilidad en la operación interna.
32	Fallas en los equipos de comunicaciones	Contratos de mantenimiento. Equipo de contingencia y aplicación de respaldos de acuerdo con las políticas definidas.
33	Fallas en los servidores (computadores principales)	Contratos de mantenimiento. Equipo de contingencia y aplicación de respaldos de acuerdo con las políticas definidas.

34	Equipo de usuario final inseguro.	Aplicación automática de políticas de seguridad por medio de Active Directory. Perfiles de usuarios limitados para instalar software y hacer modificaciones en el equipo. Losequiposseencuentranengarantía. A los equipos se les ha aplicado el Service Pack recomendado por el proveedor.
35	Ausencia de controles cruzados que comprueben la integridad de la información y el funcionamiento correcto de las aplicaciones.	Por medio del Centro de Operaciones se revisa la calidad de la información en sistemas clave.
36	Errores en la creación de usuarios y en la asignación de privilegios de acceso.	El personal que tiene a cargo la implementación de la seguridad está capacitado para estas funciones. Como parte del desarrollo de proyectos se deben definir los roles y una descripción.
37	Sistemas sin mecanismos de trazabilidad de transacciones (pistas de auditoría).	Se ha definido la utilización de pistas como parte de los estándares de programación. Se utiliza el LogMiner.
38	No se conocen los costos asignados a los servicios prestados por TI.	Se debe mejorar el registro de costos asociados a cada servicio para contar con información precisa en este sentido.
39	No se cuenta con un proceso de análisis para mejorar los costos que están asociados a los servicios de TI.	Se debe mejorar el registro de costos asociados a cada servicio para contar con información precisa en este sentido.

40	El personal no cuenta con el tiempo suficiente para recibir, de manera completa, la capacitación correspondiente.	Se informa con anticipación a las jefaturas sobre las actividades de capacitación para que se tome en cuenta en la asignación de trabajos.
41	El personal no cuenta con las actitudes y aptitudes requeridas para hacer uso de la información por medio de las soluciones automatizadas.	Periódicamente, por medio del Centro de Capacitación, se realizan charlas para fomentar la cultura informática en la institución.
42	La capacitación que se brinda a los usuarios no es efectiva para que puedan utilizar eficientemente los recursos informáticos disponibles.	Se preparan guías para la capacitación que sirva de apoyo a los estudiantes e instructores. Se preparan tutores virtuales. Se seleccionan los instructores buscando personal con facilidad de expresión.
43	No se cuenta con presupuesto para diseñar e implementar programas de capacitación para los usuarios.	Se está fomentando el uso de capacitación virtual que reduce significativamente los costos. Para esto se ha equipado al Centro de Capacitación.
44	No contar con una respuesta oportuna y efectiva para las consultas de los usuarios de TI y a la atención de los incidentes.	Utilización de un software para automatizar la presentación de los incidentes, la asignación y el seguimiento correspondiente. Manejo de niveles de prioridad por procesos y usuarios críticos para la institución.

45	Las soluciones que se aplican, ante los incidentes reportados por los usuarios, no son efectivas.	Se da capacitación a los técnicos en los nuevos productos. Se solicita al usuario que firme la solicitud de servicio cuando el trabajo está concluido.
46	Los usuarios no están informados sobre los procedimientos que se deben seguir para reportar los incidentes.	Por medio del correo electrónico frecuentemente se envían mensajes a los funcionarios recordándoles políticas y procedimientos en materia de TI.
47	No se cuenta o no se aplica el procedimiento definido para la asignación, atención y seguimiento de los incidentes.	Se cuenta con un software para gestionar las solicitudes. El personal de la USTI tiene instrucciones claras sobre el procedimiento. Se cuenta con un funcionario responsable del seguimiento.
48	No se realiza una adecuada gestión de métricas sobre los incidentes reportados y atendidos.	Se aplican encuestas a los usuarios para conocer su nivel de satisfacción y sus recomendaciones para mejorar el servicio prestado.
49	Se realizan cambios operativos que no se reflejan en la documentación.	Documentación de los procesos operativos. Actualización de guías de trabajo cuando se realizan cambios.

50	Se realizan cambios en la configuración de componentes de la infraestructura y no se reflejan en la documentación.	Se implementó una bitácora donde se registran todos los cambios realizados en la configuración de TI. Parte del procedimiento, para la aplicación de los cambios, es la actualización de la documentación correspondiente.
51	No se conoce el impacto de hacer cambios en los componentes de la configuración.	Se tiene documentada la relación de componentes de TI necesarios para la implementación y funcionamiento de los servicios clave.
52	No se aplica el procedimiento oficializado para la gestión de problemas.	Se tiene que oficializar y aplicar el proceso para la gestión de problemas.
53	No se documentan las soluciones aplicadas a los problemas.	Se está elaborando el documento para la documentación, el proveedor si lo realiza por obligación contractual
54	Hay dificultad para definir el ámbito de acción de los proveedores para la solución de problemas.	Se especifica claramente, en los carteles de los procedimientos, las responsabilidades de los proveedores y los servicios requeridos.
55	Alteración o pérdida de la información registrada en base de datos o equipos.	Periódicamente se revisan los respaldos. Se tienen definidos roles de acceso por usuario y se revisa que no exista conflicto en los roles asignados. Se revisan los programas, con mucho detalle, antes de ponerlos en producción.

56	Información desactualizada o incorrecta.	Se revisa la calidad del código generado. Se creó una dependencia de la CGR especializada en la gestión de la información. Se brinda asesoría y capacitación constante a los usuarios.
57	Acceso no autorizado a la información.	Se han definido políticas de TI con responsabilidad para los usuarios. Se ha implementado un esquema automático para que los usuarios cambien sus claves. No se gestionan claves por medios informales de comunicación.
58	Instalaciones físicas mal diseñas que pongan en peligro la integridad del equipo de cómputo y del personal.	Las instalaciones tienen puertas con control de acceso restringido. En el año 2005 se acondicionaron los sitios de trabajo para tener más visibilidad y fomentar el trabajo en equipo.
59	Acceso no autorizado al centro de cómputo.	Se cuenta con acceso restringido (por tarjeta) y cámaras de vigilancia. Se tiene una bitácora de acceso.
60	Ausencia de detectores de humo.	Está pendiente por restricciones de presupuesto.
61	Fallas en los equipos que mantienen el medio ambiente apropiado para la operación de TI (UPS, Aire acondicionado)	Se han realizado revisiones de la instalación eléctrica. Se cuenta con planta y UPS.

62	No aplicación de las políticas para la generación de respaldos.	Definición de procedimiento de contingencia para la generación de respaldos. El personal responsable debe informar cuando se presenta alguna dificultad en la generación de los respaldos.
63	No efectuar un monitoreo constante sobre la operación de la plataforma.	Se cuenta con herramienta para monitorear la red. Se cuenta con software para monitorear los servidores de aplicaciones, bases de datos y sistemas.
64	Suspensión de servicios sin seguir el procedimiento establecido.	Bitácoras de cambios en la configuración y suspensión de servicios. Se han definido procedimientos e instruido al personal.
65	No contar con un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI.	Está pendiente la definición y oficialización del procedimiento para realizar esta actividad.
66	No percibir los cambios que se realizan en el entorno.	La institución, por medio de Estrategia Institucional, mantiene un monitoreo constante sobre los cambios en el entorno. Se encarga de reflejarlos en los planes de trabajo.

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.	Se debe mejorar la definición y análisis de indicadores de TI.
68	No contar con un programa de control interno efectivo para TI que incluya auto-evaluaciones y revisiones por parte de terceros.	Se realizan las auto evaluaciones solicitadas en la Ley General de Control Interno.
69	No contar con la documentación de los procesos de TI.	Se cuenta con descripción de procesos y procedimientos. Los procesos se describen en el plan de TI.
70	Uso de software no licenciado	Los perfiles de usuario tienen restricción para la instalación de software.
71	Exceder la cantidad de usuarios autorizados para utilizar un producto licenciado.	Se lleva el inventario de licencias adquiridas y licencias instaladas. Los usuarios no tienen autorización para instalar software (se restringe por perfil de usuario en Active Directory).
72	Facilitar los medios para la instalación de software a terceros.	Se ha instruido, sobre el tema, al personal de Servicio al Cliente que tiene a cargo la gestión de medios.

73	Contar con un plan estratégico no alineado a la estrategia institucional.	El ejercicio para la definición del Plan Estratégico y sus posteriores revisiones se realizan con la participación de representantes de todas las Divisiones. Se cuenta con el apoyo y seguimiento del Despacho de las Srs. Contraloras sobre el uso de las tecnologías de información.
74	Se tiene Plan Estratégico desactualizado.	El Plan Estratégico se revisa anualmente y se ajusta cuando se realizan cambios en la planificación estratégica institucional.
75	No contar con un modelo de información del negocio que sea utilizado en la creación y actualización de los sistemas de información.	El modelo de información está documentado a nivel de las bases de datos y se cuenta con una aplicación automatizada que genera los informes.
76	Arquitectura de información desactualizada.	Se designó un funcionario para que conozca la información de la institución y valide los proyectos pero no se han establecido los controles documentales del caso.
77	Arquitectura de información no responde a la cadena de valor.	Se deben mejorar la documentación de la arquitectura de la información en función de la cadena de valor.
78	Adquisición de tecnologías que no aportan valor a la organización.	Se revisan las características de los productos de acuerdo con las necesidades de la institución.

79	Contar con equipo costoso que no cuenta con contratos de mantenimiento.	Se tiene un plan de renovación de equipo. Dentro del presupuesto se reservan las partidas correspondientes.
80	No aplicación de los canales de comunicación establecidos para informar sobre la gestión de TI.	Periódicamente se realizan reuniones informativas con todo el personal de la USTI. Igualmente se mantiene informado al Despacho sobre la evolución de los proyectos y la operativa de TI.
81	No se tienen documentados los canales de comunicación.	Está pendiente de documentarse los canales formales.
82	No se tiene dominio sobre las herramientas en uso.	Desarrollo periódico del Diagnóstico de Necesidades de Capacitación (DNC). Ejecución del programa de capacitación (de acuerdo con el disponible presupuestario).
83	Equipo de trabajo con baja motivación, poco creativo y no comprometido con el logro de los objetivos.	Se realizan dos evaluaciones de clima laboral por año. Comunicación constante sobre los planes de trabajo y compromisos de gestión. Gestión orientada al logro de los objetivos.

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.	Están definidos los estándares y procedimientos que se deben aplicar en el desarrollo de los productos. Se realizan revisiones de cumplimiento de alcance. Se aplican pruebas para identificar errores antes de liberar versiones nuevas o actualizadas de los productos de software.
85	Desarrollar productos que no cumplen con los requerimientos de calidad.	Aplicación de estándares y procedimientos de calidad. Capacitación del personal en técnicas de calidad.
86	No administrar los riesgos de TI.	Se cuenta con un plan contra contingencias. Anualmente se realiza un ejercicio de valoración de riesgos. Se aplican los instrumentos definidos para el cumplimiento del SEVRI
87	Utilizar un marco de trabajo deficiente para la gestión de riesgos, y no alineado con el apetito del riesgo institucional.	Se aplican las indicaciones del SEVRI. Se realizan auto evaluaciones de riesgos a nivel de procesos.
88	El personal no está capacitado adecuadamente para realizar una gestión efectiva de los riesgos.	Se utilizan las instrucciones definidas dentro del marco orientador del SEVRI.
89	No contar con el contenido presupuestario para la ejecución de los proyectos.	Exposición de la importancia de los proyectos en la Asamblea Legislativa para darles prioridad. Recurrir a cooperación internacional.

90	Inestabilidad en el equipo de proyecto.	Documentación de los proyectos. Divulgación del proyecto dentro del equipo. Desarrollo de talleres
91	Desarrollo de proyectos no alineados al Plan Estratégico	Planificación de proyectos de acuerdo con el PAO y la aprobación del Gerente de División Organizacional.
92	Los proyectos no están documentados	Verificación de que los proyectos cumplen con la metodología correspondiente. Validar el cumplimiento de estándares.
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.	Se cuenta con una metodología oficializada para la gestión de proyectos la cual es de aplicación obligatoria. Capacitación sobre el tema para los directores de proyecto y los ingenieros de la USTI.
94	Exceder el tiempo planificado para la ejecución de los proyectos.	Seguimiento frecuente de los proyectos (por semana). Reasignación de recursos. Fortalecer los ejercicios de planificación.
95	Falta de apoyo del patrocinador del proyecto.	Establecimiento de compromisos de gestión. Vinculación de Planes Anuales Operativos entre la USTI y unidades usuarias.

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
9	Daño físico en los equipos de la plataforma tecnológica.	1	4	4
10	Obsolescencia de la infraestructura tecnológica.	2	3	6
11	Desarrollo de sistemas y servicios que son difíciles de utilizar para el usuario.	2	3	6
12	No existe guía de usuario para el uso del sistema.	2	2	4
13	Retrasos en los procesos de contratación administrativa.	2	3	6
14	Se adquiere equipo no compatible con la infraestructura en uso.	1	3	3
15	Se adquiere equipo sin que existan talleres para la reparación y mantenimiento de los mismos.	1	3	3
16	Trabajar directamente en equipos de producción.	1	4	4
17	Versiones de software para desarrollo y producción diferentes.	1	4	4
18	No contar con la metodología y procedimientos necesarios para la administración de los cambios.	2	4	8
19	Libertad en el uso de componentes tecnológicos (software libre).	1	3	3
20	Instalación de parches sin seguir las recomendaciones del proveedor.	1	3	3
21	Ausencia de niveles de servicio aceptados que faciliten la gestión.	2	3	6
22	Definición de niveles de servicio que sobrepasan la capacidad instalada de TI.	1	3	3

23	No contar con los recursos necesarios para cumplir con los niveles de servicio.	**2**	**3**	**6**
24	No existe contrato de mantenimiento	**1**	**4**	**4**
25	Debilidad en la administración de servicios de terceros que implica que éstos no cumplan satisfactoriamente los requerimientos del negocio.	2	**3**	**6**
26	Incumplimiento de las políticas definidas por las partes.	**1**	**3**	**3**
27	Tiempo de respuesta degradado.	**1**	**3**	**3**
28	No hacer planeamiento de la capacidad.	**2**	**3**	**6**
29	Los recursos de la infraestructura tecnológica no son suficientes para atender las demandas de servicios.	1	**4**	**4**
30	Recuperación de software no es factible	**1**	**4**	**4**
31	Suspensión de servicio de Internet	**2**	**4**	**8**
32	Fallas en los equipos de comunicaciones	**2**	**3**	**6**
33	Fallas en los servidores (computadores principales)	2	**3**	**6**
34	Equipo de usuario final inseguro.	**1**	**3**	**3**
35	Ausencia de controles cruzados que comprueben la integridad de la información y el funcionamiento correcto de las aplicaciones.	**2**	**3**	**6**
36	Errores en la creación de usuarios y en la asignación de privilegios de acceso.	**1**	**4**	**4**
37	Sistemas sin mecanismos de trazabilidad de transacciones (pistas de auditoría).	1	**2**	**2**
38	No se conocen los costos asignados a los servicios prestados por TI.	**3**	**3**	**9**
39	No se cuenta con un proceso de análisis para mejorar los costos que están asociados a los servicios de TI.	**3**	**3**	**9**
40	El personal no cuenta con el tiempo suficiente para recibir, de manera completa, la capacitación correspondiente.	**1**	**3**	**3**
41	El personal no cuenta con las actitudes y aptitudes requeridas para hacer uso de la información por medio de las soluciones automatizadas.	1	**3**	**3**

42	La capacitación que se brinda a los usuarios no es efectiva para que puedan utilizar eficientemente los recursos informáticos disponibles.	**1**	**2**	**2**
43	No se cuenta con presupuesto para diseñar e implementar programas de capacitación para los usuarios.	**1**	**3**	**3**
44	No contar con una respuesta oportuna y efectiva para las consultas de los usuarios de TI y a la atención de los incidentes.	**1**	**3**	**3**
45	Las soluciones que se aplican, ante los incidentes reportados por los usuarios, no son efectivas.	1	**4**	**4**
46	Los usuarios no están informados sobre los procedimientos que se deben seguir para reportar los incidentes.	**1**	**3**	**3**
47	No se cuenta o no se aplica el procedimiento definido para la asignación, atención y seguimiento de los incidentes.	**1**	**3**	**3**
48	No se realiza una adecuada gestión de métricas sobre los incidentes reportados y atendidos.	**2**	**3**	**6**
49	Se realizan cambios operativos que no se reflejan en la documentación.	1	**4**	**4**
50	Se realizan cambios en la configuración de componentes de la infraestructura y no se reflejan en la documentación.	**2**	**4**	**8**
51	No se conoce el impacto de hacer cambios en los componentes de la configuración.	**2**	**4**	**8**
52	No se aplica el procedimiento oficializado para la gestión de problemas.	**3**	**3**	**9**
53	No se documentan las soluciones aplicadas a los problemas.	4	**5**	**20**
54	Hay dificultad para definir el ámbito de acción de los proveedores para la solución de problemas.	**1**	**3**	**3**
55	Alteración o pérdida de la información registrada en base de datos o equipos.	**1**	**4**	**4**
56	Información desactualizada o incorrecta.	**1**	**4**	**4**
57	Acceso no autorizado a la información.	1	**5**	**5**
58	Instalaciones físicas mal diseñas que pongan en peligro la integridad del equipo de cómputo y del personal.	**1**	**3**	**3**
59	Acceso no autorizado al centro de cómputo.	**2**	**3**	**6**

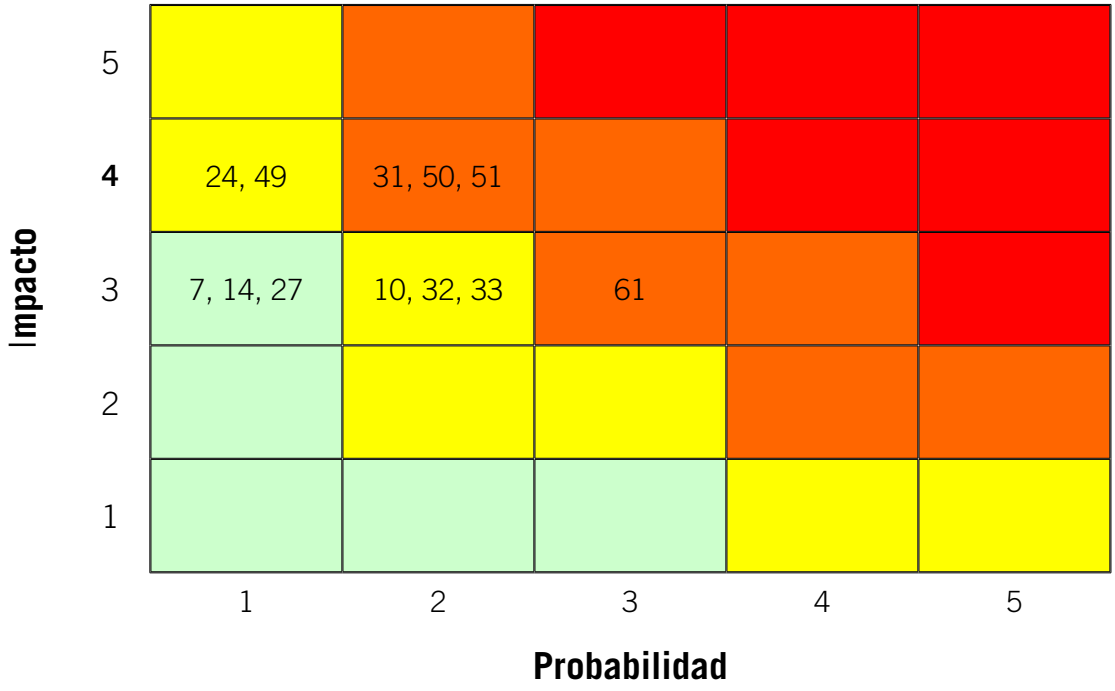
60	Ausencia de detectores de humo.	**3**	**3**	**9**
61	Fallas en los equipos que mantienen el medio ambiente apropiado para la operación de TI (UPS, Aire acondicionado)	3	**3**	**9**
62	No aplicación de las políticas para la generación de respaldos.	**1**	**4**	**4**
63	No efectuar un monitoreo constante sobre la operación de la plataforma.	**2**	**3**	**6**
64	Suspensión de servicios sin seguir el procedimiento establecido.	**2**	**3**	**6**
65	No contar con un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI.	3	**3**	**9**
66	No percibir los cambios que se realizan en el entorno.	**1**	**3**	**3**
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.	**3**	**4**	**12**
68	No contar con un programa de control interno efectivo para TI que incluya auto-evaluaciones y revisiones por parte de terceros.	**2**	**3**	**6**
69	No contar con la documentación de los procesos de TI.	1	**3**	**3**
70	Uso de software no licenciado	**1**	**3**	**3**
71	Exceder la cantidad de usuarios autorizados para utilizar un producto licenciado.	**1**	**3**	**3**
72	Facilitar los medios para la instalación de software a terceros.	**2**	**3**	**6**
73	Contar con un plan estratégico no alineado a la estrategia institucional.	1	**4**	**4**
74	Se tiene Plan Estratégico desactualizado.	**1**	**4**	**4**
75	No contar con un modelo de información del negocio que sea utilizado en la creación y actualización de los sistemas de información.	**2**	**3**	**6**
76	Arquitectura de información desactualizada.	**2**	**4**	**8**
77	Arquitectura de información no responde a la cadena de valor.	2	**3**	**6**
78	Adquisición de tecnologías que no aportan valor a la organización.	**1**	**3**	**3**

79	Contar con equipo costoso que no cuenta con contratos de mantenimiento.	**1**	**3**	**3**
80	No aplicación de los canales de comunicación establecidos para informar sobre la gestión de TI.	**1**	**2**	**2**
81	No se tienen documentados los canales de comunicación.	2	**2**	**4**
82	No se tiene dominio sobre las herramientas en uso.	**2**	**4**	**8**
83	Equipo de trabajo con baja motivación, poco creativo y no comprometido con el logro de los objetivos.	**1**	**4**	**4**
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.	**1**	**4**	**4**
85	Desarrollar productos que no cumplen con los requerimientos de calidad.	2	**3**	**6**
86	No administrar los riesgos de TI.	**2**	**4**	**8**
87	Utilizar un marco de trabajo deficiente para la gestión de riesgos, y no alineado con el apetito del riesgo institucional.	**2**	**4**	**8**
88	El personal no está capacitado adecuadamente para realizar una gestión efectiva de los riesgos.	**2**	**3**	**6**
89	No contar con el contenido presupuestario para la ejecución de los proyectos.	2	**5**	**10**
90	Inestabilidad en el equipo de proyecto.	**1**	**3**	**3**
91	Desarrollo de proyectos no alineados al Plan Estratégico	**1**	**3**	**3**
92	Los proyectos no están documentados	**2**	**4**	**8**
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.	2	**4**	**8**
94	Exceder el tiempo planificado para la ejecución de los proyectos.	**2**	**3**	**6**
95	Falta de apoyo del patrocinador del proyecto.	2	4	8

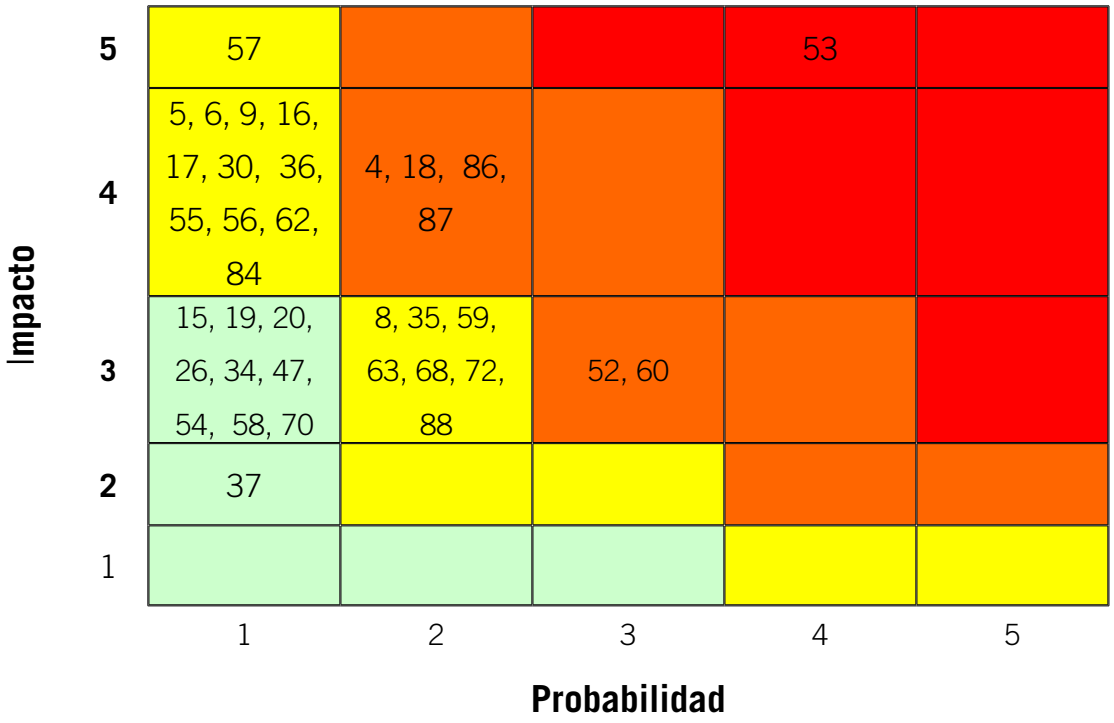
P = Probabilidad, I = Impacto, S = Severidad

Mapas térmicos riesgos controlados

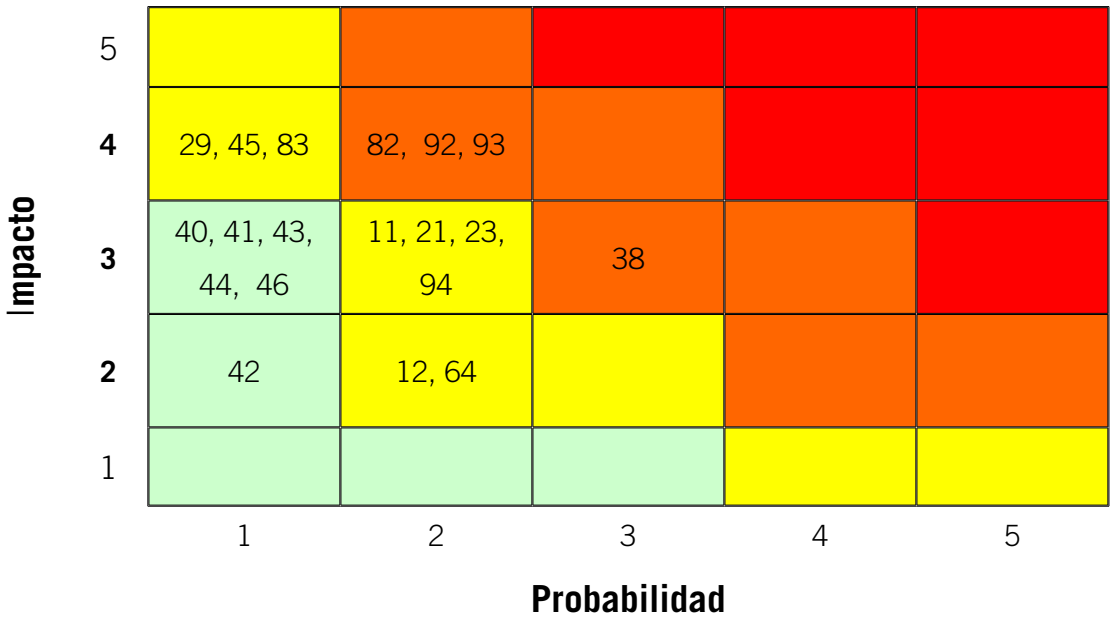
Infraestructura



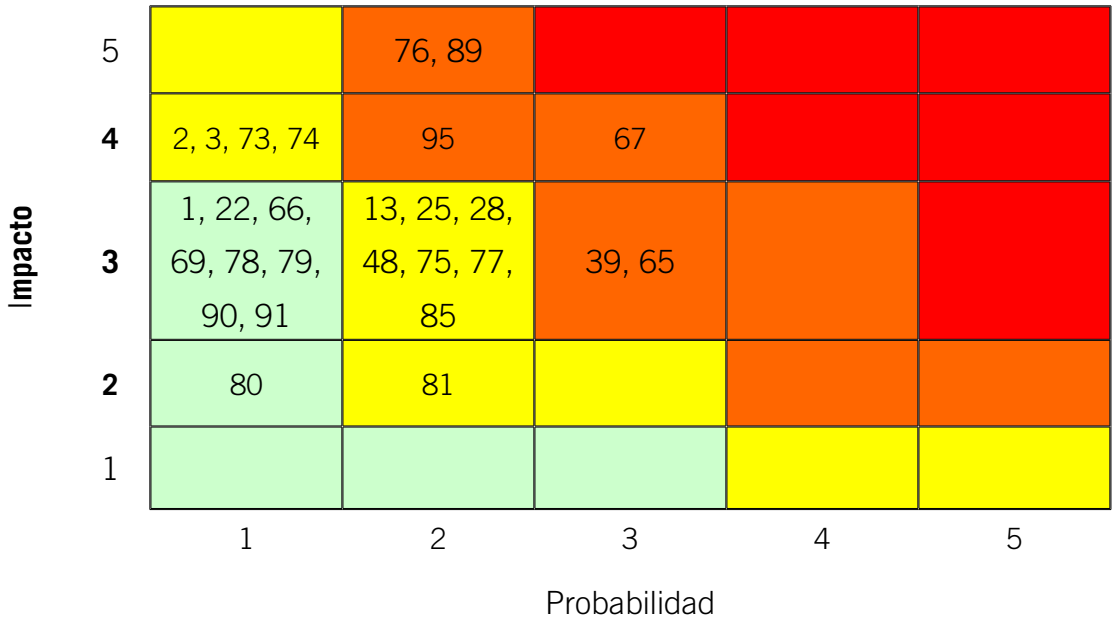
Seguridad y control



Suministro de servicios



Inserción tecnológica



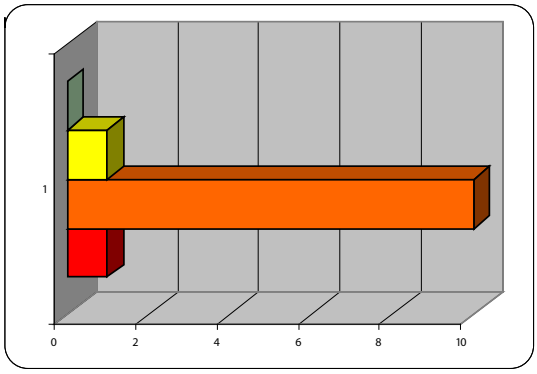
Para facilitar el análisis del nivel de riesgo de los procesos de TI se presenta en siguiente cuadro en el cual se presentan los valores totales de cantidad de riesgos, por cada proceso, en las evaluaciones de riesgos absolutos y riesgos controlados. Posteriormente esta información se presenta en gráficos y cuadros de porcentajes:

Proceso de TI	Severidad	R. Absolutos	R. Controlados
Infraestructura	Extrema	1	0
	Alta	10	4
	Moderada	1	5
	Baja	0	3
	Total de riesgos	**12**	**12**
Seguridad y control	Extrema	7	1
	Alta	22	6
	Moderada	8	19
	Baja	0	11
	Total de riesgos	**37**	**37**
Suministro de servicios	Extrema	2	0
	Alta	11	4
	Moderada	6	9
	Baja	0	6
	Total de riesgos	**19**	**19**
Inserción tecnológica	Extrema	3	0
	Alta	15	6
	Moderada	9	12
	Baja	0	9
	Total de riesgos	**27**	**27**

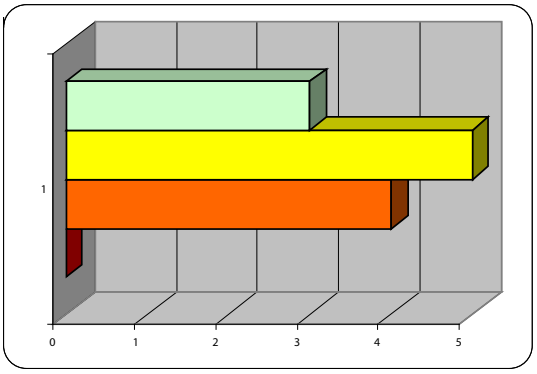
En los siguientes gráficos y cuadros se observa la evaluación de los riesgos, según cada proceso de TI, tanto a nivel absoluto como a nivel controlado. De esta manera se puede notar fácilmente el efecto de los controles en la distribución de los riesgos según su severidad la cual está representada en lo gráficos por los colores usados en los mapas térmicos.

Riesgos de infraestructura

Riesgos absolutos



Riesgos controlados

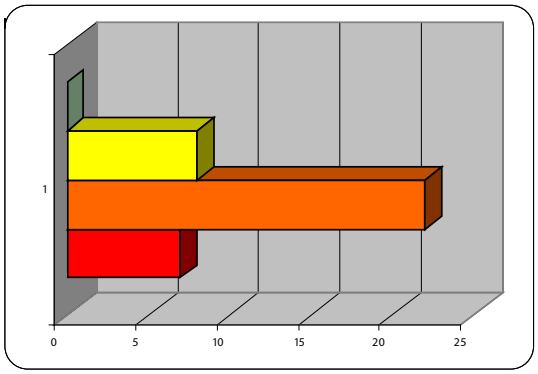


Severidad	Riesgos absolutos	Riesgos controlados
Extrema	8%	0%
Alta	84%	33%
Moderada	8%	42%
Baja	0%	25%

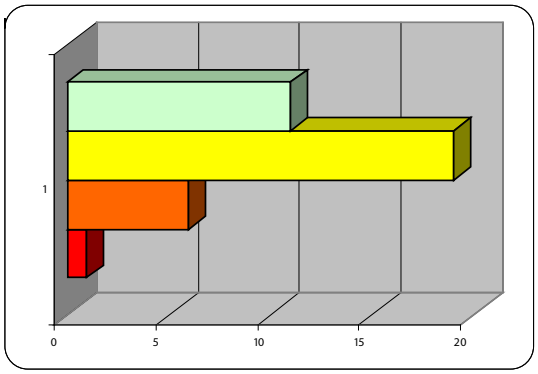
Después de valorar los controles, desde el punto de vista del proceso de infraestructura, se tienen 4 riesgos que deben ser gestionados, éstos representan el 33% de los riesgos identificados y relacionados con este proceso.

Riesgos se seguridad y control

Riesgos absolutos



Riesgos controlados

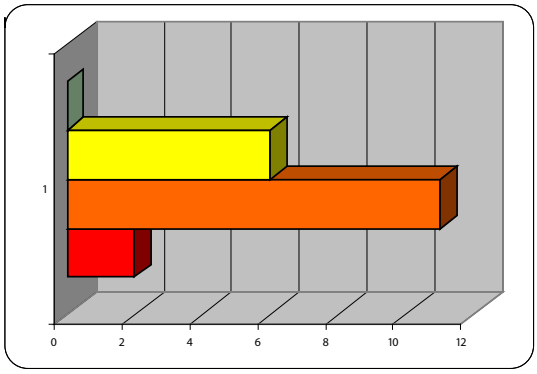


Severidad	Riesgos absolutos	Riesgos controlados
Extrema	19%	3%
Alta	59%	16%
Moderada	22%	51%
Baja	0%	30%

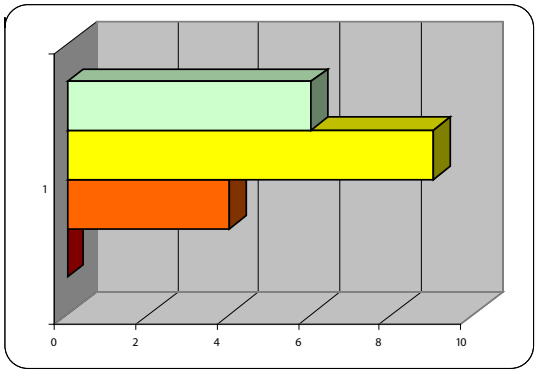
La mayor cantidad de riesgos identificados están asociados con el proceso de seguridad y control, de los 37 riesgos 7 están en las categorías de severidad extrema y alta por lo cual deben ser gestionados. Esos 7 riesgos representan el 19% de los riesgos identificados. Es importante notar que en la valoración de riesgos absolutos la cantidad el porcentaje de riesgos clasificados en esa categoría es de 78% lo cual significa que la aplicación de los controles colaboró, de manera muy importante, para reducir la cantidad de riesgos cuya severidad es extrema y alta.

Riesgos de suministro de servicios

Riesgos absolutos



Riesgos controlados

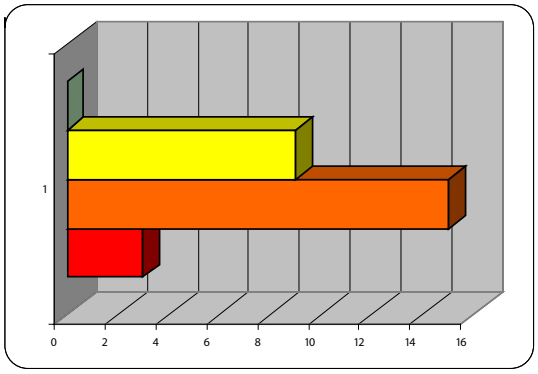


Severidad	Riesgos absolutos	Riesgos controlados
Extrema	11%	0%
Alta	57%	21%
Moderada	32%	47%
Baja	0%	32%

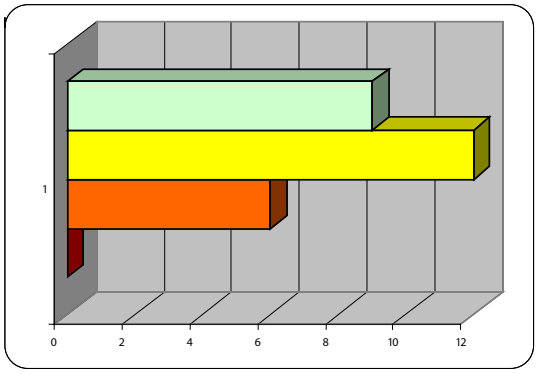
En la calificación de riesgos absolutos el 78% de los riesgos identificados (en total 19 para el proceso de suministro de servicios) se encuentran con calificación de severidad extrema o alta. En la segunda calificación, considerando la aplicación de los controles actuales, en la calificación de riesgos con severidad extrema se tiene 4%, eso representa el 21% de los riesgos identificados para el proceso.

Riesgos de inserción tecnológica

Riesgos absolutos



Riesgos controlados



Severidad	Riesgos absolutos	Riesgos controlados
Extrema	11%	0%
Alta	56%	22%
Moderada	33%	45%
Baja	0%	33%

En cuanto al proceso de inserción tecnológica se identificaron 27 riesgos, es el segundo proceso en cantidad de riesgos identificados. De estos riesgos el 67% tienen una calificación absoluta con severidad extrema y alta. Después de calificarlos, tomando en cuenta la aplicación de los controles actuales, este porcentaje baja a 22% que corresponde a 6 riesgos con calificación de severidad alta.

Valoración del nivel de riesgo de los procesos

Es importante conocer la calificación global de riesgo que tiene cada proceso tanto a nivel en la calificación de riesgos absolutos como de riesgos controlados; este valor se obtuvo con el promedio de la calificación de exposición (impacto * probabilidad) para los riesgos en cada proceso. Los resultados son los siguientes:

Proceso de TI	Riesgos absolutos	Riesgos controlados
Infraestructura	10.9	5.7
Seguridad y control	10.6	5.2
Suministro de servicios	9.3	5.0
Inserción tecnológica	8.9	5.4
En promedio	9.9	5.3

Se puede notar fácilmente que la calificación de los procesos es muy similar, a nivel de riesgos absolutos los procesos de infraestructura así como de seguridad y control son los que tienen las calificaciones más altas a nivel de severidad promedio de sus riesgos. En vista de que para los cuatro procesos de TI la calificación está entre 8 y 12 les corresponde un nivel promedio de severidad de alta (representada en color anaranjado). En cuanto a los riesgos controlados también la calificación es muy similar para todos los procesos, en este caso son los procesos de infraestructura e inserción tecnológica los que tienen las calificaciones mayores. Todos los procesos tienen calificaciones que están entre 4 y 6 por lo cual se ubican en nivel moderado como promedio de severidad de sus riesgos que se representan en color amarillo. Según estás calificaciones la situación de los procesos es muy similar tanto a nivel de riesgos absolutos como de riesgos controlados; esto quiere decir que los controles están orientados a gestionar los riesgos de manera equitativa.

Riesgos prioritarios

Después de realizar el análisis de riesgos y determinar su nivel de severidad tanto en la calificación de riesgos absolutos como de riesgos controlados se ha determinado que los siguientes riesgos son de prioritaria atención:

Id	Descripción del riesgo	Proceso de TI relacionado
4	Versiones de software desactualizadas.	Seguridad y control
18	No contar con la metodología y procedimientos necesarios para la administración de los cambios.	Seguridad y control
31	Suspensión de servicio de Internet	Infraestructura
38	No se conocen los costos asignados a los servicios prestados por TI.	Suministro de servicios
39	No se cuenta con un proceso de análisis para mejorar los costos que están asociados a los servicios de TI.	Inserción tecnológica
50	Se realizan cambios en la configuración de componentes de la infraestructura y no se reflejan en la documentación.	Infraestructura
51	No se conoce el impacto de hacer cambios en los componentes de la configuración.	Infraestructura
52	No se aplica el procedimiento oficializado para la gestión de problemas.	Seguridad y control
53	No se documentan las soluciones aplicadas a los problemas.	Seguridad y control
60	Ausencia de detectores de humo.	Seguridad y control

61	Fallas en los equipos que mantienen el medio ambiente apropiado para la operación de TI (UPS, Aire acondicionado)	Infraestructura
65	No contar con un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI.	Inserción tecnológica
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.	Inserción tecnológica
76	Arquitectura de información desactualizada.	Inserción tecnológica
82	No se tiene dominio sobre las herramientas en uso.	Suministro de servicios
86	No administrar los riesgos de TI.	Seguridad y control
87	Utilizar un marco de trabajo deficiente para la gestión de riesgos, y no alineado con el apetito del riesgo institucional.	Seguridad y control
89	No contar con el contenido presupuestario para la ejecución de los proyectos.	Inserción tecnológica
92	Los proyectos no están documentados	Suministro de servicios

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.	Suministro de servicios
95	Falta de apoyo del patrocinador del proyecto.	Inserción tecnológica

Planes de tratamiento

A continuación se indican los planes de acción para cada uno de los riesgos cuya evaluación de severidad, a nivel de riesgos controlados, fue de extrema o alta:

Id	Descripción del riesgo	Planes de acción
4	Versiones de software desactualizadas.	Se presupuestaron las partidas para contratar el mantenimiento y se incluyó en el PAO la actividad para actualización de plataforma. En el diagnóstico de capacitación se incorporó la capacitación necesaria.
18	No contar con la metodología y procedimientos necesarios para la administración de los cambios.	Con base al manual de normas técnicas sobre tecnologías de información, se revisará y actualizará el método para administración de los cambios
31	Suspensión de servicio de Internet	En el presupuesto del 2008 se incluyó el alquiler de un canal alterno al proveedor actual del servicio para la solución de fallas locales en el ISP

38	No se conocen los costos asignados a los servicios prestados por TI.	Se desarrollará un modelo de costos para conocer el costo por servicios o productos
39	No se cuenta con un proceso de análisis para mejorar los costos que están asociados a los servicios de TI.	En paralelo al modelo de costos se realizará el modelo para el análisis respectivo
50	Se realizan cambios en la configuración de componentes de la infraestructura y no se reflejan en la documentación.	Se enfatizará en el personal la obligación de actualizar la documentación con los cambios que se realicen a la infraestructura
51	No se conoce el impacto de hacer cambios en los componentes de la configuración.	Se coordinarán los cambios previo a realizarlos para proyectar el impacto, incluyendo de ser posible al proveedor
52	No se aplica el procedimiento oficializado para la gestión de problemas.	Se realizará un taller para analizar las razones por las cuales no se aplica en algunos casos el procedimiento, y para generar las acciones correctivas
53	No se documentan las soluciones aplicadas a los problemas.	Se incluyó como parte del manual para continuidad de la operación, la obligación de documentar soluciones aplicadas para el mejoramiento continuo.
60	Ausencia de detectores de humo.	Sin incluyó en el presupuesto del 2008 la adquisición de la solución

61	Fallas en los equipos que mantienen el medio ambiente apropiado para la operación de TI (UPS, Aire acondicionado)	El CC mantiene una UPS exclusiva para equipos críticos y se compró una adicional para respaldo de las tres que soportan toda la institución. Se está elaborando el procedimiento institucional para soporte de medio ambiente.
65	No contar con un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI.	A partir del 2008 se aplicará un nuevo método de evaluación del desempeño basado en compromisos de desempeño
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.	Con base a los planes tácticos y la nueva cartera de proyectos se rediseñaron los indicadores para medir el desempeño
76	Arquitectura de información desactualizada.	Se tiene programada la revisión de la arquitectura para ajustarla de ser necesario, con base a la nueva cartera de proyectos
82	No se tiene dominio sobre las herramientas en uso.	Se desarrollará la capacitación necesaria para que el personal utilice las herramientas adecuadamente
86	No administrar los riesgos de TI.	Se establecerán administradores de riesgos por área de coordinación, y reuniones mensuales de seguimiento para auto evaluación y mejora

87	Utilizar un marco de trabajo deficiente para la gestión de riesgos, y no alineado con el apetito del riesgo institucional.	Se lleva a cabo estudio de auditoría, se desarrollo un sistema automatizado para control de riesgos, y se está realizando una evaluación de riesgos.
89	No contar con el contenido presupuestario para la ejecución de los proyectos.	Ajustar la cartera de proyectos al presupuesto aprobado y elaborar un presupuesto extraordinario para reprogramar los proyectos en caso de que este se apruebe
92	Los proyectos no están documentados	Se harán auditorias periódicas para control de los expedientes de sistemas
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.	Se acordó capacitar en el 2008 a todos los gerentes sobre la necesidad de aplicar la metodología, e iniciar cada proyecto capacitando a todo el equipo de proyecto
95	Falta de apoyo del patrocinador del proyecto.	A partir de la nueva cartera de proyectos, los gerentes de División tienen que asegurar los recursos a los proyectos en los cuales son patrocinadores; total o compartido, e incluirlos como parte de su PAO

Evaluación de riesgos tratados

En la siguiente tabla se presenta la calificación de los riesgos proyectando la aplicación de los planes de tratamiento (riesgos tratados):

Id	Riesgo	P	I	S
4	Versiones de software desactualizadas.	1	3	3
18	No contar con la metodología y procedimientos necesarios para la administración de los cambios.	1	4	4
31	Suspensión de servicio de Internet	2	2	4
38	No se conocen los costos asignados a los servicios prestados por TI.	1	3	3
39	No se cuenta con un proceso de análisis para mejorar los costos que están asociados a los servicios de TI.	1	3	3
50	Se realizan cambios en la configuración de componentes de la infraestructura y no se reflejan en la documentación.	1	4	4
51	No se conoce el impacto de hacer cambios en los componentes de la configuración.	1	4	4
52	No se aplica el procedimiento oficializado para la gestión de problemas.	2	3	6
53	No se documentan las soluciones aplicadas a los problemas.	1	5	5
60	Ausencia de detectores de humo.	2	3	6
61	Fallas en los equipos que mantienen el medio ambiente apropiado para la operación de TI (UPS, Aire acondicionado)	2	3	6
65	No contar con un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI.	1	3	3
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.	1	3	3
76	Arquitectura de información desactualizada.	1	4	4
82	No se tiene dominio sobre las herramientas en uso.	1	3	3
86	No administrar los riesgos de TI.	1	4	4
87	Utilizar un marco de trabajo deficiente para la gestión de riesgos, y no alineado con el apetito del riesgo institucional.	1	4	4

89	No contar con el contenido presupuestario para la ejecución de los proyectos.	1	5	**5**
92	Los proyectos no están documentados	1	4	**4**
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.	1	3	**3**
95	Falta de apoyo del patrocinador del proyecto.	1	4	**4**

Es interesante observar la evolución de los riesgos en cada uno de los niveles de evaluación (absoluto, controlado y tratado); seguidamente se presenta la calificación para los riesgos prioritarios.

ID	Riesgo	Absoluto	Controlado	Tratado
4	Versiones de software desactualizadas.	**12**	**8**	**3**
18	No contar con la metodología y procedimientos necesarios para la administración de los cambios.	12	**8**	**4**
31	Suspensión de servicio de Internet	**12**	**8**	**4**
38	No se conocen los costos asignados a los servicios prestados por TI.	**9**	**9**	**3**
39	No se cuenta con un proceso de análisis para mejorar los costos que están asociados a los servicios de TI.	**9**	**9**	**3**
50	Se realizan cambios en la configuración de componentes de la infraestructura y no se reflejan en la documentación.	12	**8**	**4**
51	No se conoce el impacto de hacer cambios en los componentes de la configuración.	**12**	**8**	**4**
52	No se aplica el procedimiento oficializado para la gestión de problemas.	**9**	**9**	**6**

53	No se documentan las soluciones aplicadas a los problemas.	20	20	5
60	Ausencia de detectores de humo.	9	9	6
61	Fallas en los equipos que mantienen el medio ambiente apropiado para la operación de TI (UPS, Aire acondicionado)	15	9	6
65	No contar con un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI.	9	9	3
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.	12	12	3
76	Arquitectura de información desactualizada.	12	8	4
82	No se tiene dominio sobre las herramientas en uso.	12	8	3
86	No administrar los riesgos de TI.	16	8	4
87	Utilizar un marco de trabajo deficiente para la gestión de riesgos, y no alineado con el apetito del riesgo institucional.	16	8	4
89	No contar con el contenido presupuestario para la ejecución de los proyectos.	10	10	5
92	Los proyectos no están documentados	16	8	4
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.	16	8	3
95	Falta de apoyo del patrocinador del proyecto.	16	8	4

Organización para la gestión de los riesgos

A efectos de mantener una organización adecuada para la Gestión de los Riesgos en la USTI, y con el objetivo de mantener riesgos actualizados, controlados, y planes de tratamiento para mitigarlos, se adecua la organización mediante asignar un asistente de la jefatura que recopile riesgos en un nivel preliminar, los procese, y para que actualice el mapa térmico para conocimiento de la jefatura y los coordinadores de área.

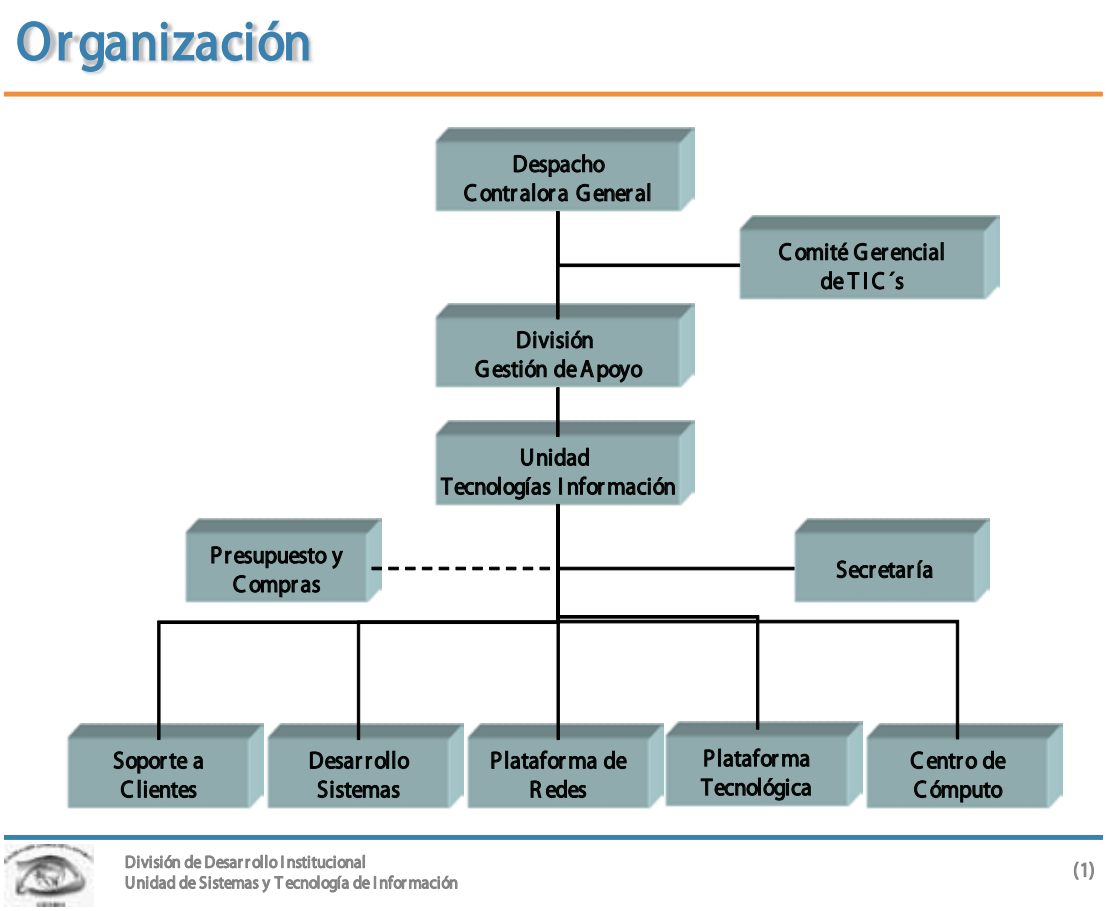
La identificación y evaluación de los riesgos debe ser sustentado por un sistema participativo de planificación que considere la misión y la visión institucionales, así como objetivos, metas y políticas; por esa razón se estarán realizando reuniones una vez al mes con los coordinadores de área para considerar el tema.

Se reforzará la administración basada en riesgos para los coordinadores de área y asistente de la jefatura, con el objetivo que darle robustez a la organización y a la UTI en su gestión, siempre bajo el modelo de administración de riesgos de la CGR, la política de valoración de riesgos emitida por el Despacho, la metodología para valoración de riesgos, y los lineamientos generados por la División de Estrategia Institucional.

Los insumos para la identificación de riesgos estarán basados principalmente en los que a continuación se indican:

- Planes institucionales, sectoriales y nacionales.
- Análisis del entorno interno y externo.
- Evaluaciones institucionales.
- Descripción de la organización (procesos, presupuesto, sistema de control interno).
- Normativa externa e interna asociada con la proceso/proyecto e institución.
- Documentos de operación diaria y de la evaluación periódica.

A continuación se incluye el organigrama de la UTI; según la propuesta en donde se identifica al asistente de la jefatura, y a los coordinadores en su último nivel.



Recomendaciones

Con base en el análisis de Administración Basada en Riesgos, llevado a cabo en la Unidad de Tecnologías de Información, se derivan una serie de recomendaciones que se incorporan a continuación en el presente documento.

a. Mantener un mapa térmico actualizado con los riesgos controlados que están identificados con una severidad alta o extrema.

b. Desarrollar una reunión cada primer lunes de mes, para que la jefatura de la UTI evalúe con los coordinadores de área los planes de tratamiento que se están aplicando a los riesgos del mapa térmico identificados como alto o extremo, con el objetivo de actualizarlos si se considera que es factible mejorarlos para mitigar el riesgo.

c. Fortalecer la administración basada en riesgos en los niveles de coordinación, mediante capacitación periódica y con base en los análisis que se realicen en las reuniones los días lunes primero de mes.

d. Centralizar la actualización preliminar de los riesgos identificados, controlados, y planes de tratamiento, en un asistente de la jefatura de UTI que se encargará de preparar el material de la reunión de los lunes, y de alertar a la jefatura inmediatamente, en caso de que se detecte un nuevo riesgo que clasifique como alto o severo.

e. Preparar al asistente de la jefatura para que procese los nuevos riesgos con fines de clasificarlos, para alertar a la jefatura en caso de riesgos extremos o altos.

f. Cada coordinador de área debe administrar con base a los riesgos detectados, reportando al asistente los nuevos riesgos detectados, mitigados, o nuevos controles que han sido aplicados, a fin de mantener la administración de riesgos actualizada; sin importar para este caso el nivel de riesgo; todos deben ser reportados para procesarlos.

g. Adquisición de un software institucional que facilite la administración basada en riesgos.