

**FONDO DE RETIRO AHORRO Y PRÉSTAMO (FRAP) - CCSS**

---

**Carta de Gerencia TI 2021**

**Informe Final**

San José, 21 de enero del 2022.

Señores  
Fondo de Retiro Ahorro y Préstamo (FRAP) - CCCSS  
Centro de Gestión Informática

Estimados señores:

Según nuestro contrato de servicios, efectuamos la visita de auditoría externa del periodo 2021 al FRAP - CCSS y con base en el examen efectuado, observamos ciertos aspectos referentes al sistema de control interno y procedimientos de Tecnología de Información, basados en los estándares establecidos según los Objetivos de Control para Información y Tecnología Relacionada – CobiT®, los cuales sometemos a consideración de ustedes en esta carta de gerencia CG TI 2021.

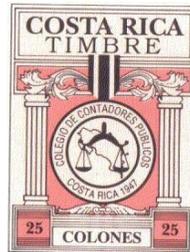
Considerando el carácter de pruebas selectivas en que se basa nuestro examen, ustedes pueden apreciar que se debe confiar en métodos adecuados de comprobación y de control interno, como principal protección contra posibles irregularidades que un examen basado en pruebas selectivas puede no revelar, si es que existiesen. Las observaciones no van dirigidas a funcionarios o colaboradores en particular, sino únicamente tienden a fortalecer el sistema de control interno y los procedimientos relacionados con las Tecnologías de Información.

Es importante señalar que la estructura de control interno establecida, incluyendo los procedimientos de control para la actividad sujeta a evaluación, son de entera responsabilidad de la administración del FRAP-CCSS.

La auditoría no está diseñada para detectar todas las deficiencias en los procesos y objetivos de control evaluados, ya que no se lleva a cabo de forma continua durante el período de revisión; las evaluaciones realizadas consisten en un estudio sustentado en muestras y pruebas selectivas de la evidencia que respalda el cumplimiento de los procesos y objetivos de control evaluados, los cuales, producto de sus limitaciones inherentes, pueden presentar resultados fallidos debido a errores o debilidades propias del control interno que ocurran y no sean detectadas. Lo anterior deja manifiesto que los eventos subsecuentes a este informe están sujetos al riesgo de que los controles establecidos se tornen inadecuados, producto de cambios en las condiciones del FRAP-CCSS.

La auditoría realizada fue requerida por la administración del FRAP-CCSS, producto de lo anterior, los resultados expresados en el presente informe son de carácter confidencial y deben ser utilizados exclusivamente por las personas autorizadas para tal fin.

**DESPACHO CARVAJAL & COLEGIADOS  
CONTADORES PÚBLICOS AUTORIZADOS**



Lic. Ricardo Montenegro Guillén  
Contador Público Autorizado N° 5607  
Póliza de Fidelidad No. 0116 FIG7  
Vence el 30 de setiembre del 2022.



“Timbre de Ley número 6663 por ¢25 del Colegio de Contadores Públicos Autorizados de Costa Rica, se adhiere y cancela en el original”

## CONTENIDO

ORIGEN DEL ESTUDIO .....	5
ALCANCE .....	5
OBJETIVO DEL ESTUDIO .....	5
PERIODO DE LA AUDITORÍA.....	6
LIMITACIONES DEL ESTUDIO.....	6
METODOLOGÍA .....	6
HALLAZGOS .....	7
MATRIZ DE SEGUIMIENTO A HALLAZGOS EMITIDOS EN CARTAS DE GERENCIA ANTERIORES .....	8
CARTA DE GERENCIA 2018.....	8
APÉNDICE .....	14
APENDICE I. VALORACIÓN DEL NIVEL DE SATISFACCIÓN SOBRE LA CALIDAD FUNCIONAL DE ALGUNOS DE LOS SISTEMAS DE INFORMACIÓN EN EL FRAP.....	14
OBJETIVO.....	14
RESULTADOS.....	14
Información sobre el sistema de información .....	15
Opinión sobre el servicio brindado por el Departamento De TIC.....	18
Cobertura de necesidades actuales .....	21
Comentarios adicionales .....	22

## **ORIGEN DEL ESTUDIO**

Como parte de la evaluación de los estados financieros del FRAP-CCSS, realizamos una evaluación de los controles generales de la gestión de tecnología de información, con el objetivo de medir el grado de riesgo de la información en lo que respecta a seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica.

La evaluación la realizamos basados en los Objetivos de Control de Tecnologías de Información (COBIT por sus siglas en inglés) emitidos por la “Information Systems Audit and Control Association” (ISACA por sus siglas en inglés) y en general las mejores prácticas de la industria de tecnología de información.

## **ALCANCE**

En esta visita el trabajo fue enfocado principalmente a las siguientes áreas:

1. Verificación del control interno en materia tecnológica con base en la normativa interna establecida, sobre los siguientes aspectos:
  - a. Planificación.
  - b. Gestión de seguridad de la información: administración de usuarios, accesos y vulnerabilidades, políticas de seguridad.
  - c. Gestión de activos y servicios de TI.
  - d. Respaldos y recuperación de información.
  - e. Gestión de cambios.
  - f. Sistemas de información.
  - g. Gestión de riesgos de TI.
  - h. Gestión de personal de TI.
2. Seguimiento a recomendaciones emitidas en periodos anteriores en materia tecnológica.

## **OBJETIVO DEL ESTUDIO**

1. Establecer un entendimiento integral del FRAP-CCSS, así como de la plataforma tecnológica que soporta sus operaciones y documentación asociada.
2. Con el propósito de cumplir con los requerimientos estipulados en la Norma Internacional de Auditoría 315, Entendiendo de la realidad y su entorno y evaluación de representación errónea de importancia relativa y en la Norma Internacional de Auditoría 330, Procedimientos del auditor en respuesta a los riesgos evaluados, evaluamos la gestión de las tecnologías de información del FRAP-CCSS.

## **PERIODO DE LA AUDITORÍA**

El estudio se realizó durante el mes de enero del 2022, corresponde a la auditoría del periodo 2021.

## **LIMITACIONES DEL ESTUDIO**

Durante el proceso de auditoría externa efectuado no se presentaron limitaciones.

## **METODOLOGÍA**

Para llevar a cabo este trabajo se utilizó una modalidad de análisis de la información suministrada por el Centro de Gestión Informática y de otras Áreas del FRAP-CCSS. Además, se formularon preguntas sobre la existencia de controles informáticos, en todos los casos necesarios solicitamos a los funcionarios las evidencias en documentos en formato digital que respaldaran sus afirmaciones.

## HALLAZGOS

No se identificaron hallazgos nuevos para el periodo evaluado.

## MATRIZ DE SEGUIMIENTO A HALLAZGOS EMITIDOS EN CARTAS DE GERENCIA ANTERIORES

Los siguientes hallazgos fueron emitidos producto de auditorías externas de periodos anteriores.

CARTA DE GERENCIA 2018	
<b>HALLAZGO 01: DEFICIENCIAS EN LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. RIESGO MEDIO.</b>	
RECOMENDACIÓN	<p><i>A la Dirección de Tecnologías de Información y Comunicaciones:</i></p> <ol style="list-style-type: none"> <li>1. Revisar y valorar la actual política seguridad de la información y demás procedimientos y normas referentes a la seguridad de modo que se actualicen con base en un análisis de riesgos. Esta revisión y actualización se debe realizar al menos una vez al año.</li> <li>2. Realizar revisiones periódicas para verificar el cumplimiento de la política de seguridad de la información en el FRE, de modo que se pueda identificar las principales deficiencias sobre la misma e implementar las medidas adecuadas, entre ellas la capacitación de los usuarios en caso de ser requerido.</li> <li>3. Presentar la actualización de los documentos sobre seguridad de la información ante la Comité Gerencial de Tecnologías de Información de modo que se realice la respectiva aprobación y divulgación.</li> </ol>
COMENTARIO DE ADMINISTRACIÓN	<p>Mediante oficio DFRE-2019-1126 con fecha 16/12/2019 Se traslada a la DTIC para su respectivo descargo. Se recibe oficio DTIC-0304-2020, se realizará la coordinación al respecto para la atención y buscar la atención del enunciado, en proceso, por lo anterior se envía oficio GF-DFRE-2020-0649 (DTIC-AudExter).pdf con fecha 11/09/2020 Se traslada a la DTIC para su respectiva revisión y descargo.</p> <p>Se recibe oficio GG-DTIC-5831-2020. El cual cita textual, (Esta Dirección, advierte que cualquier informe de auditoría llámese interno o externo debe ser discutido con el usuario. En el caso concreto se debió realizar el análisis con esta Dirección, sin embargo, no se dio, la situación se agrava porque esta unidad no comparte ni considera que sea una sana práctica que la Dirección de Tecnologías de</p>

	<p>Información y Comunicaciones deba establecer políticas de seguridad de la información cuando es un rol que le corresponde al negocio. Dado lo anterior, es importante el espacio y discusión como lo establecen las sanas prácticas en auditoría para señalar los elementos expuestos. En ese sentido esta Dirección está imposibilitada para darle atención a dicha recomendación, por ser una competencia del negocio)</p> <p>Mediante oficio DFRAP-2021-0645 (DFRAP-DTIC-AudExterna).pdf con fecha 29/10/2021 Se traslada a la DTIC para su respectivo descargo.</p> <p>Se recibe oficio GG-DTIC-0150-2022 con fecha 11/01/2022. El cual cita textual, (Traslado oficio GF-DFRAP-0645-2021 para la atención de las recomendaciones de la Auditoría Externa al Fondo de Retiro de los Empleados de la Caja Costarricense de Seguro Social FRE). De los avances sobre el tema se estará informando en informes posteriores.</p>
ESTADO	<p style="text-align: center;"><b>EN PROCESO</b></p> <p>No se suministró evidencia de la divulgación de las políticas de seguridad. Además, la política de seguridad presenta fecha del periodo 2007 y las normas de seguridad presentan fecha del 2008, lo cual refleja que no han recibido una actualización periódica tal como se establece en el punto 3 de la política de seguridad informática.</p>
<p><b>HALLAZGO 02: AUSENCIA DE UN LINEAMIENTO PARA LA EVALUACIÓN DE CONTROL INTERNO DE TI EN EL FRAP. RIESGO MEDIO.</b></p>	
RECOMENDACIÓN	<p><b><u>A la administración del FRAP:</u></b></p> <ol style="list-style-type: none"> <li>1. Establecer un lineamiento para evaluar el control interno de TI, donde se incluya:             <ol style="list-style-type: none"> <li>a. Objetivo.</li> <li>b. Regulaciones.</li> <li>c. Descripción de la metodología.</li> <li>d. Responsabilidad.</li> <li>e. Seguimiento.</li> <li>f. Políticas y procedimientos abarcados.</li> <li>g. Informes de control.</li> </ol> </li> </ol>

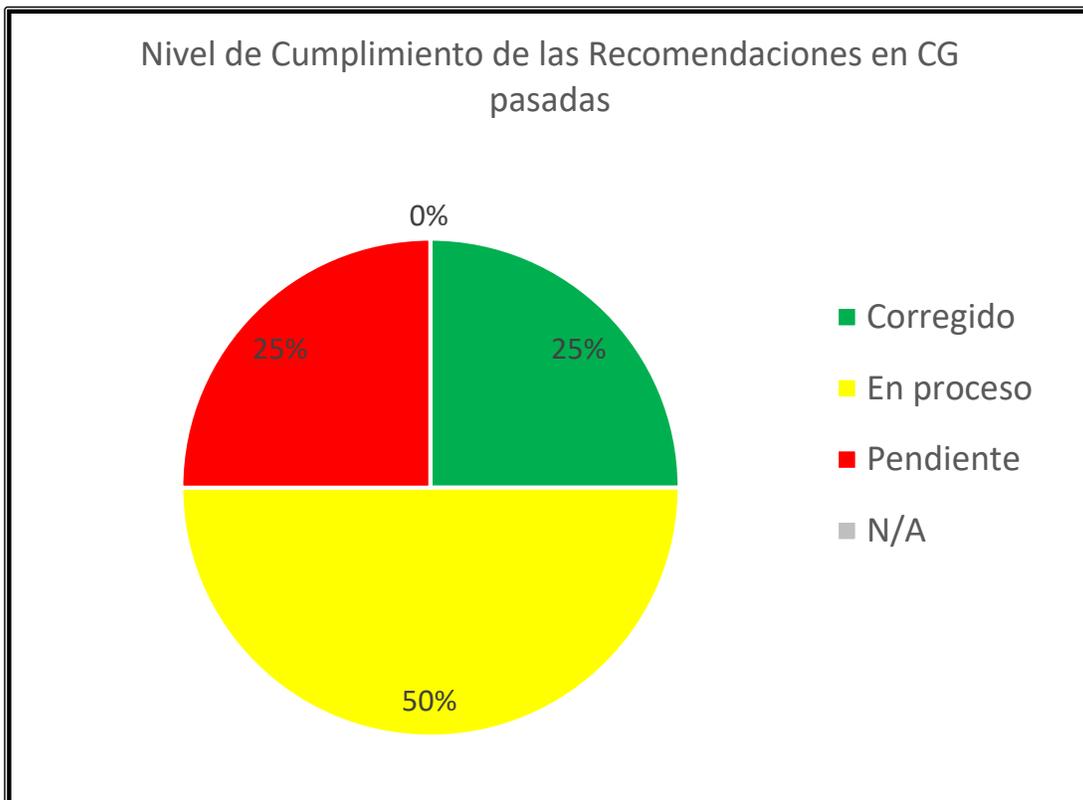
	<p>2. Cumplir con el lineamiento establecido, realizar las evaluaciones periódicamente y documentar las inconsistencias detectadas.</p> <p>3. Realizar los planes de acción necesarios para corregir las inconsistencias detectadas.</p> <p>La administración del FRAP debe de garantizar la implementación del lineamiento establecido en materia de control interno de TI.</p>
<p>COMENTARIO DE ADMINISTRACIÓN</p>	<p>Mediante oficio DFRAP-2019-1126 con fecha 16/12/2019 Se traslada a la DTIC para su respectivo descargo.</p> <p>Se recibe oficio DTIC-0304-2020, se realizará la coordinación al respecto para la atención y buscar la atención del enunciado, en proceso, por lo anterior se envía oficio GF-DFRAP-2020-0649 (DTIC-AudExter).pdf con fecha 11/09/2020 Se traslada a la DTIC para su respectiva revisión y descargo.</p> <p>Se recibe oficio GG-DTIC-5831-2020. El cual cita textual (... es importante para esta Dirección aclararle a la Auditoría Externa tal como lo indica la Ley de Control interno en su artículo N° 10, es responsabilidad del titular subordinado el control interno de la unidad sobre la cual preside. Ante la figura expresada por la Ley, la Dirección de Tecnologías de Información y comunicaciones no puede ejercer la figura de control Interno al equipo de tecnologías del FRAP...)</p> <p>Valorar con la Auditoría Externa, que el FRE en materia de tecnologías no tiene una unidad especializada ya que depende a nivel estructural al Centro de Gestión Informática de la Gerencia Financiera que a su vez es precedido por la Dirección de tecnologías de Información y Comunicaciones de la Caja Costarricense de Seguro Social, los aspectos de regulaciones, metodologías, políticas y procedimientos de T.I. son regulados por la Dirección de tecnologías institucional.</p> <p>Mediante oficio DFRAP-2021-0645 (DFRAP-DTIC-AudExterna).pdf con fecha 29/10/2021 Se traslada a la DTIC para su respectivo descargo.</p> <p>Se recibe oficio GG-DTIC-0150-2022 con fecha 11/01/2022. El cual cita textual, (Traslado oficio GF-DFRAP-0645-2021 para la atención de las recomendaciones de la Auditoría Externa al Fondo de Retiro de los Empleados de la</p>

	Caja Costarricense de Seguro Social FRE). De los avances sobre el tema se estará informando en informes posteriores.
ESTADO	<b>EN PROCESO</b>  Para el hallazgo en cuestión se indica en los comentarios de la administración que, la atención está en proceso al 11 de enero del 2022 y que se estará dando seguimiento para informes posteriores.
<b>HALLAZGO 03: DEFICIENCIAS EN LA GESTIÓN DE LICENCIAS DE SOFTWARE DEL FRAP. RIESGO BAJO.</b>	
RECOMENDACIÓN	<p><u><i>A la Dirección de Tecnologías de Información y Comunicaciones:</i></u></p> <ol style="list-style-type: none"> <li>1. Mantener un inventario de licencias adquiridas en el FRAP de modo que se tenga un control de las licencias que se encuentran disponibles y/o en uso.</li> <li>2. Mantener un control del software instalado en cada una de las terminales de los usuarios del FRAP, de modo que se puede verificar en cualquier momento que software poseen los equipos de los usuarios.</li> </ol> <p>Verificar periódicamente si el software instalado en los equipos se encuentra dentro de la lista de software permitido por la institución y si las licencias utilizadas se encuentran bajo control de la DTIC. En caso de identificar software no permitido o licencias no controladas, se debe realizar un proceso de mantenimiento para desinstalar dichos programas.</p>
COMENTARIO DE ADMINISTRACIÓN	<p>Mediante la herramienta institucional SCCM (System Center Configuration Manger) con la aplicación CCSS Enterprise Remote Access / Configuration Manager Control en el reporte (Software 02E - Installed software on a specific computer) se brinda el respectivo seguimiento y control periódico al software instalado en cada computadora.</p> <p>Se evidenció la existencia de software instalado el cual no se encuentra dentro de la lista de software permitido, entre ellos se identificaron CyberLink PowerDVD y Foxit PhantomPDF. Se realizaron las medidas correctivas, a pesar de que el software mencionado anteriormente es software libre. Atendido al 14/01/2022</p>
ESTADO	<b>CORREGIDO</b>  Por medio de la herramienta institucional SCCM (System Center Configuration Manager) es posible realizar un seguimiento y control periódicos del software instalado en los equipos. Se realizaron medidas correctivas para el software que no se encuentra autorizado por el FRAP, el cual fue desinstalado de las computadoras. Hay una

	herramienta que proporciona control para el software no permitido, pero no existe un manual o procedimiento que muestre el procedimiento a seguir para las medidas correctivas. Además, de acuerdo con las normas de seguridad solo los usuarios con perfil administrador y destacados del CGI tienen la autorización para instalar software en los equipos, por tanto, se asegura que las herramientas utilizadas por los colaboradores son las aceptadas por el FRAP.
<b>Carta de Gerencia 2017, 2016 y 2015</b>	
<b>1. Necesidades de TIC del FRAP no contempladas en la estrategia.</b>	
RECOMENDACIÓN	Continuar con la ejecución del debido proceso iniciado por la Dirección del Fondo de Retiro, Ahorro y Préstamo. Una vez que éste se dé por aprobado es necesario que se realicen todas las actividades pertinentes que garanticen la debida gestión de la TIC, alineando ésta con las necesidades del negocio.
COMENTARIO DE ADMINISTRACIÓN	Pendiente de Atender al 18-08-2020. Pendiente de Atender al 16-09-2020. Pendiente de Atender al 29-10-2021. Pendiente de Atender al 14-01-2022.
ESTADO	<b>PENDIENTE</b>
	Para el hallazgo en cuestión se indica en los comentarios de la administración que, la atención sigue pendiente al 14 de enero del 2022, por ende, no fue posible verificar acciones aplicadas al respecto y el estado se deja en pendiente.

Se resume a continuación el cumplimiento de las recomendaciones emitidas en informes de auditorías anteriores:

ESTADO	2015,2016 y 2017	2018	TOTAL POR ESTADO
<b>CORREGIDOS</b>	0	1	1
<b>EN PROCESO</b>	0	2	2
<b>PENDIENTES</b>	1	0	1
<b>N/A</b>	0	0	0
<b>TOTAL POR AÑO</b>	<b>1</b>	<b>3</b>	<b>4</b>



*Resultados del nivel de cumplimiento de las recomendaciones en Cartas de Gerencia anterior*

## APÉNDICE

### APENDICE I. VALORACIÓN DEL NIVEL DE SATISFACCIÓN SOBRE LA CALIDAD FUNCIONAL DE ALGUNOS DE LOS SISTEMAS DE INFORMACIÓN EN EL FRAP

#### OBJETIVO

Medir el nivel de satisfacción que posee el usuario con respecto al (los) sistema (as) que utiliza FRAP, y al soporte que brinda el Departamento de Tecnologías de Información.

#### RESULTADOS

A continuación, se muestra el resultado de la evaluación realizada con respecto a la calidad funcional de algunos de los sistemas de información implantados en, según la percepción de los usuarios finales.

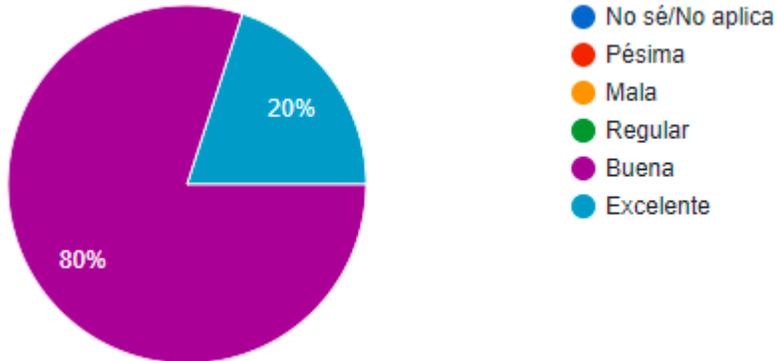
En total, cinco colaboradores de la institución brindaron respuesta, las áreas de trabajo a las cuales pertenecen son; Dirección FRAP, Subárea de Inversiones, Subárea Contable FRAP. Los sistemas de información evaluados, así como la cantidad de respuestas por cada uno, se muestran en la tabla siguiente:

Sistema por Valorar	Cantidad de respuestas
Sistema Integrado FRA	2
Sistema Gestión de Inversiones	1
Sistema Integrado del FRAP SIFRAP	2

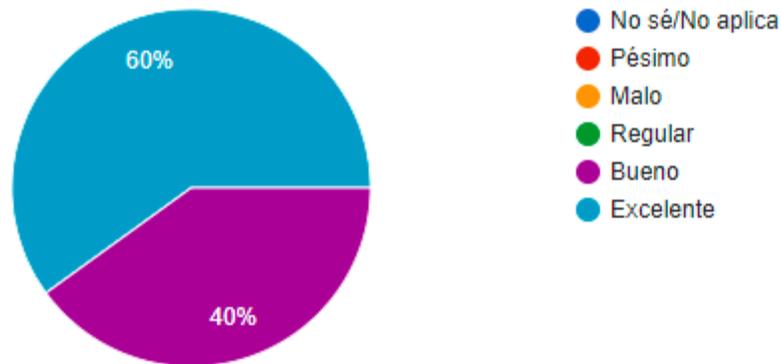
En los siguientes apartados, se muestran las respuestas registradas según la sección evaluada.

## Información sobre el sistema de información

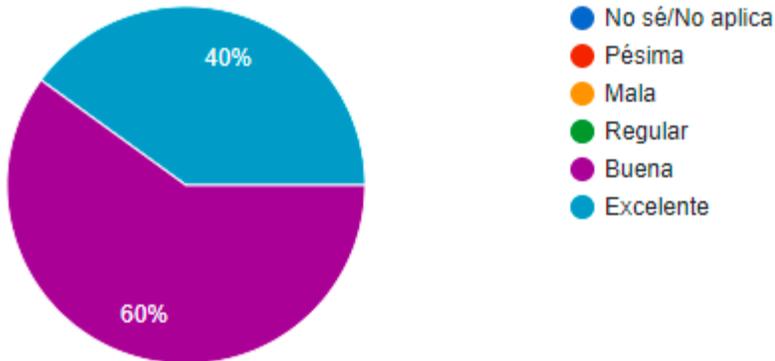
### 1. Exactitud de los datos



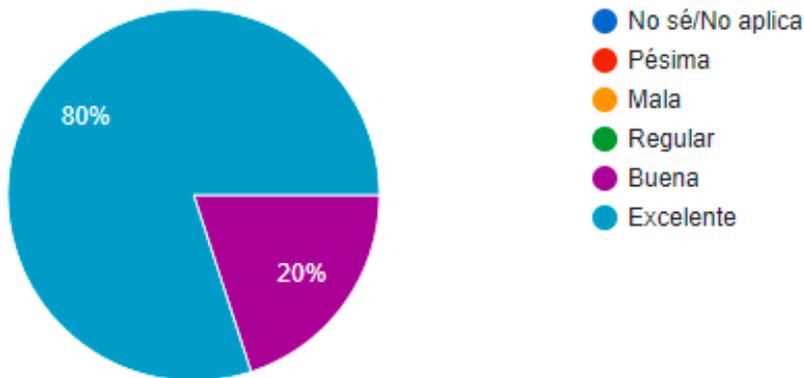
### 2. Contenido de la información



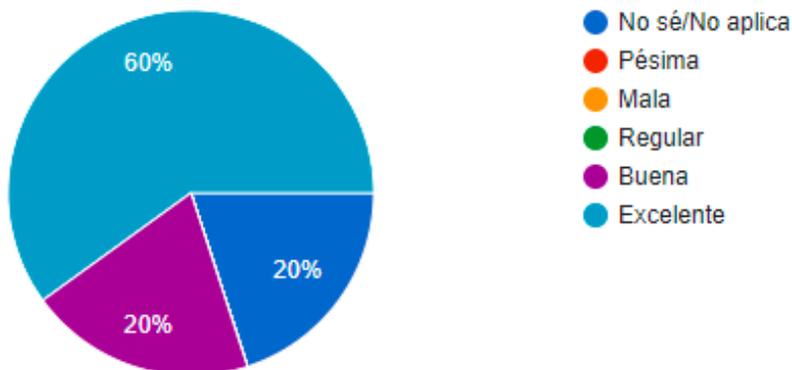
### 3. Calidad de la información



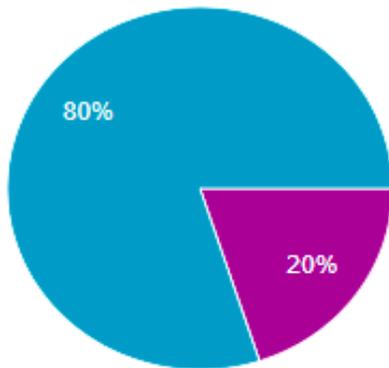
**4. Entrega de resultados**



**5. Seguridad de la información**

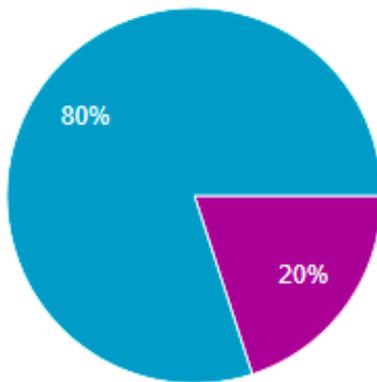


**6. Fiabilidad del sistema**



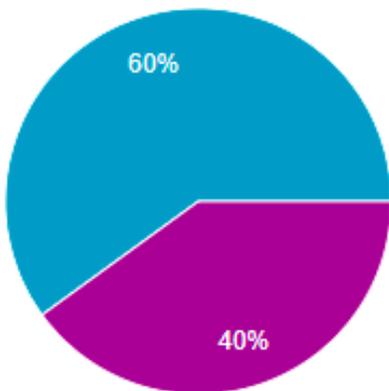
- No sé/No aplica
- Pésima
- Mala
- Regular
- Buena
- Excelente

### 7. Facilidad de uso



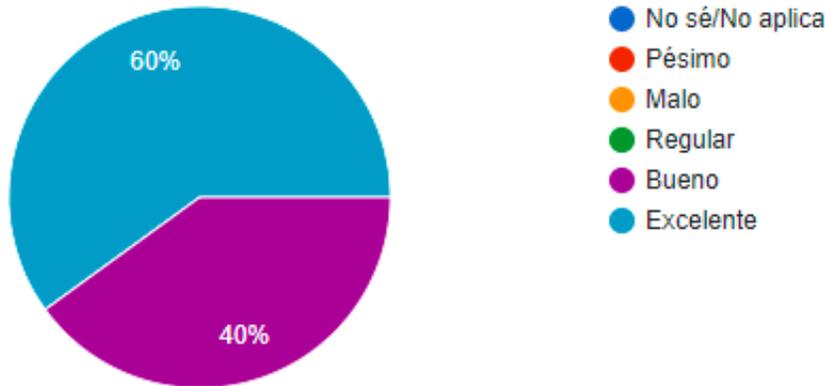
- No sé/No aplica
- Pésima
- Mala
- Regular
- Buena
- Excelente

### 8. Documentación



- No sé/No aplica
- Pésima
- Mala
- Regular
- Buena
- Excelente

## 9. Reportes especiales



En los gráficos anteriores es posible apreciar que para los atributos de; contenido de información, entrega de resultados, seguridad de la información, fiabilidad del sistema, facilidad de uso, documentación y reportes especiales, predomina la respuesta “Excelente”, lo cual representa una percepción muy favorable por parte de los usuarios.

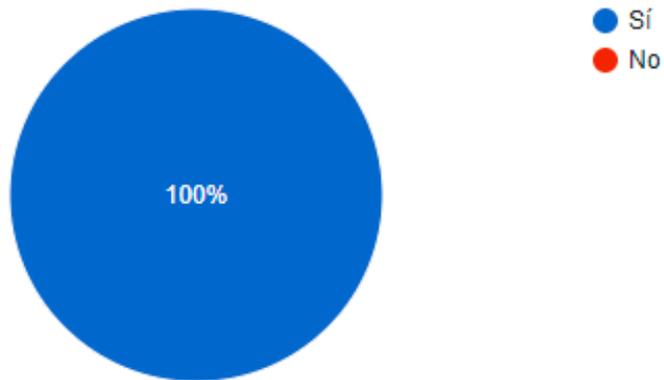
Para los casos de; exactitud de los datos y calidad de la información, predomina la respuesta “Buena”. Es viable prestar atención a estas respuestas ya que, es posible que existan oportunidades de mejora sin explotar y que mejorarían la experiencia de los usuarios.

Por otra parte, se consultó a los usuarios cuáles nuevas funcionalidades pueden ser implementadas en los sistemas, dando como respuestas;

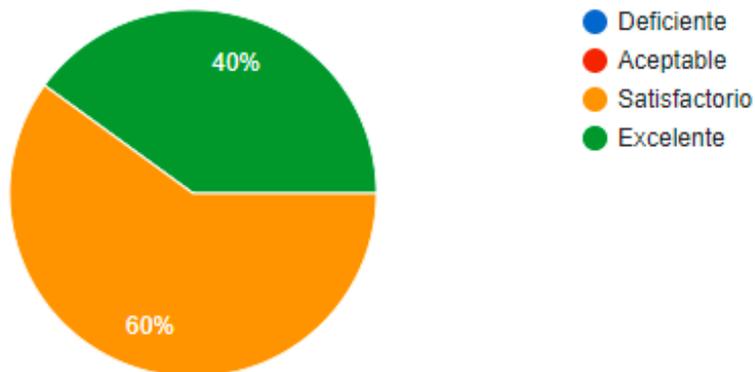
- “Añadir más gráficos”
- “Mas reportes por ejemplo de los otros fondos (FAP, FRIP, FOCARE) y toda su parte contable, ya se está trabajando de hecho”
- “Se ha estado trabajando en la creación de diferentes fondos, en donde la implementación del sistema a un fondo en particular causo modificaciones o alteraciones en el ya existe”

### Opinión sobre el servicio brindado por el Departamento De TIC

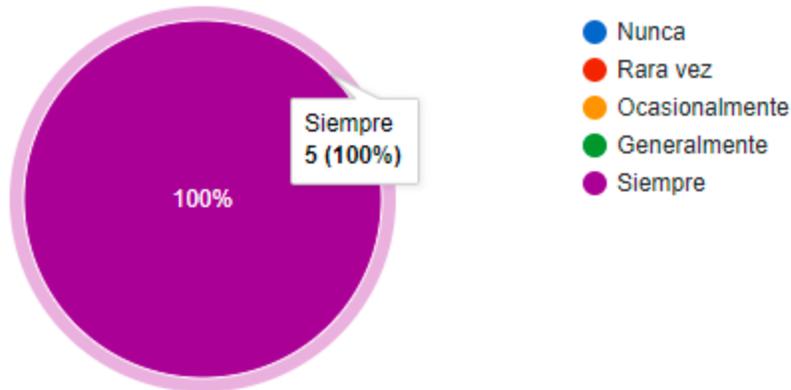
**Departamento de TI brinda los resultados esperados**



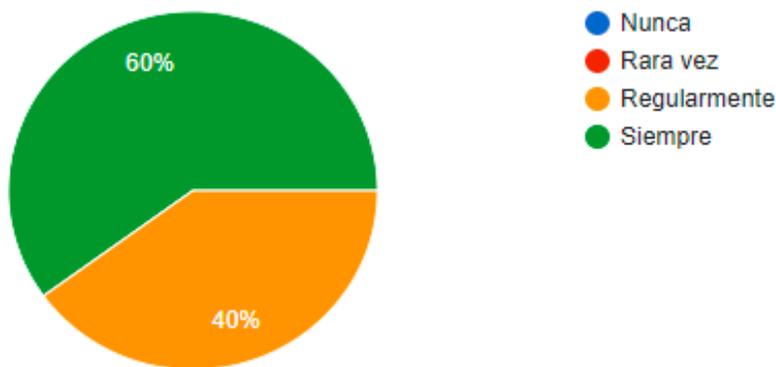
### Servicio proporcionado por el Departamento de TI



### Disponibilidad del Departamento de TI para atender nuevos requerimientos



### Entrega puntual de los trabajos solicitados al Departamento de TI



Los gráficos anteriores reflejan que la opinión de los usuarios con respecto al servicio que brinda TI es Aceptable. El 100% de los usuarios que contestaron, consideran que TI brinda los resultados esperados.

Para la entrega puntual de los trabajos un 40% considera que se cumple regularmente y un 60% que los trabajos siempre son entregados. Es decir 3, de los 5 usuarios que contestaron están satisfechos con la puntualidad de las entregas.

Con respecto a la disponibilidad para atender nuevos requerimientos, el 100% de los usuarios que contestaron consideran que siempre está disponible.

Como parte de las respuestas ampliadas brindadas por los usuarios, destaca que; el soportado dado al FRAP es excelente y siempre están anuentes a colaborar y brinda atención oportuna.

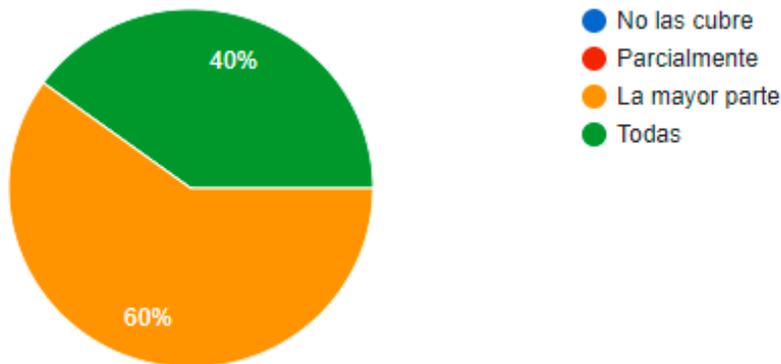
Específicamente sobre el servicio brindado, los usuarios indican que siempre están en disposición de ayudar en cualquier momento, sin embargo, mencionan que a veces se retrasan un poco con las respuestas a errores.

Sobre la disponibilidad, las opiniones coinciden en que, “Existe un cronograma de trabajo al que se le da seguimiento a la atención de nuevos requerimientos de manera oportuna”.

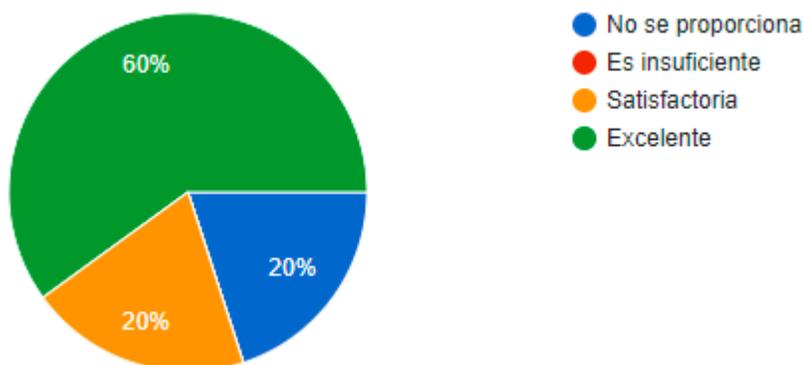
Para el caso de la puntualidad, las opiniones coinciden en que; “Existe compromiso de atender oportunamente, principalmente las urgencias, pero a veces existen atrasos”.

### Cobertura de necesidades actuales

#### Cobertura de necesidades con el sistema de información proporcionado por el Departamento de TI



#### Capacitaciones recibidas en materia informática



Los resultados anteriores reflejan que las necesidades de los usuarios con respecto al (los) sistema (as) utilizado (os) se cubren en un 60% la mayor parte del tiempo y un 40% todas. Es viable analizar cuáles necesidades no están siendo del todo cubiertas, el por qué y buscar una solución

En materia de capacitación los resultados se dividen; un 60% considera que son excelentes, un 20% refleja que son satisfactorias y otro 20% considera que no se proporcionan. Es viable analizar si es necesario aumentar la cantidad de capacitaciones que se brindan, en pro de mejorar la calidad de los servicios.

### **Comentarios adicionales**

Como opiniones adicionales, los usuarios indican que:

- Cuando se realicen requerimientos de contabilidad, tienen que ir muy de la mano de los procesos de la subárea de inversiones, es decir falta todavía más coordinación entre ambas unidades.
- Establecer evaluaciones periódicas entre usuarios e ingenieros con el fin de solventar consultas y refrescamientos de la operativa y mejorar resultados de esta, es decir, fortalecer el control interno.
- Cuando se presenta un error y este corregido, que sea corregido a partir del momento en que sea solucionado y no dar cierto tiempo a que aparezca el mismo error.