INFORME NRO. **DFOE-BIS-IF-00001-2021**
27 de mayo, 2021

INFORME DE LA AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA FUNCIONALIDAD Y OPERACIÓN DEL SISTEMA NACIONAL DE INFORMACIÓN Y REGISTRO ÚNICO DE BENEFICIARIOS (SINIRUBE)

2021

CONTENIDO

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Resumen Ejecutivo

¿QUÉ EXAMINAMOS?

La auditoría de carácter especial tuvo por objeto determinar si la operación del Sistema Nacional de Información y Registro Único de Beneficiarios del Estado (SINIRUBE) es conforme a los objetivos de su creación, al marco normativo y las buenas prácticas relativas a la operación y mantenimiento de sistemas de información. Para lo cual, se evaluaron controles específicos relacionados con procesos de Tecnologías de Información (TI) críticos como lo son los vinculados a la gestión de servicios, y operaciones computacionales de procesamiento de información, entre otros.

¿POR QUÉ ES IMPORTANTE?

La ley de creación del SINIRUBE así como su reglamento le confieren una serie de obligaciones y responsabilidades a este Órgano, siendo una de las más relevantes ofrecer una metodología única para determinar los niveles de pobreza. En la práctica, ello derivó en el desarrollo e implementación de una herramienta automatizada (con alcance nacional) para asistir en el proceso de toma de decisiones para la asignación de beneficios de parte del Estado. De manera que existen alrededor de 78 instituciones públicas usuarias del sistema, con al menos 42 programas sociales integrados; los cuales se ven beneficiados en su utilización para establecer las asignaciones de ayudas que se realizan sobre la base de la información allí contenida.

¿QUÉ ENCONTRAMOS?

En la auditoría realizada, en lo que respecta a operaciones de TI, se encontró que el 95% (75/79) de las instituciones usuarias del sistema no están cumpliendo con su obligación de remitir de manera periódica la información que alimenta el sistema, de acuerdo con lo estipulado en los convenios entre partes. El SINIRUBE carece de controles que permitan garantizar la actualización de la información en tiempo y forma. Al respecto, el 32,1% (68/211) de los usuarios del sistema perciben que la información allí contenida no está debidamente actualizada.

Por otra parte, el SINIRUBE siendo un órgano desconcentrado del Instituto Mixto de Ayuda Social (IMAS), aporta información al Sistema Específico de Valoración de Riesgos (SEVRI) de esa institución, sin que cuente con un proceso propio de valoración de riesgos en materia de tecnologías de información y procesos de negocio, lo cual limita la priorización de objetivos y/o proyectos en materia de TI. Así, la última valoración que consta fue efectuada por una empresa externa en el 2019.

Asimismo, el 50% (98/196) de los encuestados indicaron desconocer las herramientas de reporte de fallas del sistema, un 74,5% (147/196) desconoce acerca de la existencia del mecanismo de ayuda al usuario (mesa de servicio), mientras que el 85,2% (167/196) señaló no contar con manuales que detallen las funcionalidades del sistema.

Finalmente, se determinó que la Administración no implementa procesos de gestión de la capacidad de su plataforma tecnológica, ni se realizan proyecciones de necesidad de crecimiento de sus equipos principales, por ende, aun cuando se señala que su estructura

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

actual no es suficiente para el cumplimiento del plan estratégico, no se conoce la brecha real de lo requerido para garantizar el crecimiento y expansión del sistema.

¿QUÉ SIGUE?

Con el propósito de fortalecer la gestión de tecnologías de información del SINIRUBE, y de facilitar la labor de las instituciones usuarias del sistema, se giran disposiciones a la Dirección Ejecutiva, para que se implementen mecanismos de control con el propósito de fortalecer dicha gestión y facilitar la labor de las instituciones usuarias del sistema. Asimismo, se le dispone que implementen controles relacionados con la entrega oportuna de información por parte de las instituciones de acuerdo a lo estipulado en los convenios suscritos, así como los controles operativos que regulen la recepción y actualización de información en el sistema.

Por último, se deberán implementar procesos de atención de incidentes y consultas y gestión de riesgo, y en cuanto a la gestión de capacidad de sus equipos principales, implementar un proceso periódico de diagnóstico que le permita identificar las necesidades técnicas, materiales, humanas y de información del SINIRUBE.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

1. Introducción

ORIGEN DE LA AUDITORÍA

1.1. El estudio se efectuó con fundamento en las competencias que le confieren a la Contraloría General de la República (CGR) los artículos 183 y 184 de la Constitución Política, 12 y 21 de su Ley Orgánica, N.º 7428.

1.2. El Instituto Mixto de Ayuda Social se crea con el fin de resolver o al menos tratar el problema de la pobreza extrema en el país, de tal suerte que se le concede la administración de recursos que provienen de fuentes públicas y privadas y que se buscan apoyar a la clase social más vulnerable.

1.3. Creado según la Ley 4760 del 30 de abril de 1971, el IMAS depende de un conjunto de instituciones públicas con las cuales debe coordinar esfuerzos en aras de definir lo que se entiende por pobreza, pobreza extrema, riesgo social y en consecuencia articular esfuerzos para atender las diferentes necesidades de la población que en última instancia recibirá los beneficios derivados de los 46 programas sociales que integran la estrategia de lucha contra la pobreza.

1.4. Gestionar recursos para hacerlos llegar a una población debidamente pre seleccionada es una tarea que requiere de información oportuna y actualizada para tomar decisiones y orientar correctamente los recursos disponibles; es necesario que se conozcan detalladamente las características de los beneficiarios y en ese contexto se crea por medio de la Ley 9137 el SINIRUBE como mecanismo integrador entre los participantes del sistema y como un registro único de beneficiarios del Estado.

1.5. El rol del IMAS y de las instituciones que le acompañan en el ejercicio de sus labores es crítico para el desarrollo del país y más importante aún, para la población en condición de pobreza; el servicio prestado por estas instituciones toca las fibras más sensibles de la población como lo son la población infantil y los adultos mayores por citar dos casos.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

1.6. Es por eso que resulta importante realizar una valoración de las prestaciones técnicas del SINIRUBE para determinar si efectivamente este sistema cumple con los requerimientos de las diversas partes interesadas y si el sistema como medio de centralización de información para la toma de decisiones alcanza su objetivo de proveer una fuente de consulta única y efectiva para garantizar que los recursos disponibles se distribuyen de la forma más racional posible entre los ciudadanos que lo necesitan.

1.7. Toda acción que tienda a mejorar las prestaciones técnicas, operativas y de cumplimiento del SINIRUBE aporta valor a los ciudadanos, en particular a aquellos en condición de riesgo. Los fondos públicos orientados a los programas sociales son limitados y por ende optimizar su uso resulta imprescindible para alcanzar los fines que el Estado persigue en materia de disminución de la pobreza.

OBJETIVOS

1.8. El estudio tiene por objetivo determinar si la operación del SINIRUBE es conforme a los objetivos de su creación, al marco normativo y las buenas prácticas relativas a la operación y mantenimiento de sistemas de información.

ALCANCE

1.9. El estudio evaluó los controles aplicados por la administración para operar el sistema, aquellos relacionados con la seguridad de la información así como el uso que hace de dicha información, en el periodo comprendido entre el 01 de enero 2019 al 30 de junio 2020; el cual puede ampliarse en caso de que se estime necesario.

CRITERIOS DE AUDITORÍA

1.10. Los criterios de auditoría fueron enviados formalmente al señor Erickson Álvarez Calonge en su calidad de Director Ejecutivo de SINIRUBE y se comunicaron mediante oficio DFOE-DL-1109 (17735) del 11 de noviembre 2020. Al respecto no se recibieron observaciones.

METODOLOGÍA APLICADA

1.11. La auditoría se realizó de conformidad con las Normas Generales de Auditoría para el Sector Público, con el Manual General de Fiscalización Integral de la CGR y el Procedimiento de Auditoría vigente, establecido por la DFOE.

1.12. Para la elaboración de esta auditoría se utilizaron las técnicas y procedimientos estipulados en el Manual General de Fiscalización Integral (MAGEFI) de la Contraloría General de la República. Además, se observó en lo atinente, las disposiciones contenidas en las Normas Generales de Auditoría para el Sector Público (NGASP), y demás normativa aplicable.

1.13. Para el desarrollo de esta auditoría se utilizó la información suministrada en las entrevistas a funcionarios del SINIRUBE, así como las respuestas a varios requerimientos de información que se distribuyeron, tanto al Área de Tecnologías de Información como a la Auditoría Interna. Asimismo, se realizó una visita de campo al Centro de Procesamiento de Datos ubicado en el Mall San Pedro.

1.14. En la etapa de examen se aplicó un cuestionario que permitió recopilar información sobre la funcionalidad del sistema, nivel de satisfacción del usuario y su relación con el SINIRUBE a nivel de servicio, entre otros. Se aplicó en la forma de una consulta, en la que se participó al 100% de usuarios (976), de los cuales 211 dieron respuesta.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

1.15. Además se tuvo acceso al sistema mediante una cuenta temporal para cada miembro del equipo, con lo que se realizaron pruebas varias, tanto de funcionalidad, esquema de reportes y de seguridad, así como una revisión de los niveles de acceso a la información que se encuentran definidos en los perfiles.

1.16. Si bien el ejercicio de auditoría permitió evaluar tres aspectos diferentes del quehacer informático, en este informe se atiende el particular de funcionalidad y operaciones y en documento aparte se reportan las oportunidades de mejora que corresponden a seguridad de la información.

ASPECTOS POSITIVOS QUE FAVORECIERON LA EJECUCIÓN DE LA AUDITORÍA

1.17. Como parte de los aspectos positivos a resaltar, se encuentra la colaboración prestada por parte de la Administración y en particular su equipo de TI, además del apoyo de la Auditoría Interna del IMAS.

LIMITACIONES QUE AFECTARON LA EJECUCIÓN DE LA AUDITORÍA

1.18. En la aplicación de la consulta a los usuarios del sistema se tuvo dificultades para obtener respuestas, aun cuando se remitieron diversos recordatorios y se realizaron esfuerzos para contactar a los responsables correspondientes dentro de las instituciones que contaban con una mayor cantidad de usuarios.

GENERALIDADES ACERCA DEL OBJETO AUDITADO

1.19. El SINIRUBE es un órgano de desconcentración máxima con personalidad jurídica instrumental para el logro de sus objetivos, adscrito al Instituto Mixto de Ayuda Social (IMAS).

1.20. A este órgano se le asigna por ley el deber de mantener una base de datos actualizada y de cobertura nacional, eliminar duplicidad de las acciones interinstitucionales, proponer una metodología para determinar niveles de pobreza y simplificar y reducir trámites a solicitantes de beneficios. La base de datos de la institución debe permitir establecer un control sobre los programas sociales, disponer de datos oportunos, veraces y precisos, y garantizar que los beneficios lleguen a los sectores más necesitados de la sociedad.

1.21. A su vez, el SINIRUBE cuenta con un Consejo Rector, el cual está integrado por los jerarcas o representantes de instituciones como el Instituto Mixto de Ayuda Social, el Patronato Nacional de la Infancia, el Ministerio de Educación Pública, el Ministerio de Salud, la Caja Costarricense de Seguro Social, el Ministerio de Vivienda, el Instituto Nacional de Aprendizaje, el Ministerio de Trabajo y Seguridad Social y el Ministerio de Planificación Nacional y Política Económica.

COMUNICACIÓN PRELIMINAR DE LOS RESULTADOS DE LA AUDITORÍA

1.22. Los resultados de la auditoría se presentaron verbalmente el día 28 de abril de 2021 por medio de la plataforma Google Meet administrada por CGR, con la participación de los señores: Erickson Álvarez Calonge, Director Ejecutivo de SINIRUBE; Juan Luis Bermúdez Madriz, Presidente del Consejo Rector del SINIRUBE; Francisco Delgado Jiménez, Viceministro de Desarrollo Humano e Inclusión Social; Gabriela Carvajal, Asesora Jurídica, IMAS-SINIRUBE; Marianela Navarro Romero, Auditora Interna a.i.; Wady Alfaro, Auditor Interno en TI y Natalia Rojas Canales, Profesional en Informática.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

1.23. Mediante oficio DFOE-SOC-0341 (N°06227) del 30 de abril de 2021 se remitió al Lic. Juan Luis Bermúdez Madriz Presidente del Consejo Rector del SINIRUBE y al MATI Erickson Álvarez Calonge Director Ejecutivo del SINIRUBE el borrador del informe, con el propósito de que a más tardar el 7 de mayo de los corrientes se formularan y remitieran a la Gerencia del Área de Fiscalización para el Desarrollo del Bienestar Social, las observaciones que consideraran pertinentes sobre su contenido. Al respecto, mediante oficio IMAS-SINIRUBE-233-2021 de fecha 13 de mayo de 2021, se recibieron observaciones al borrador del informe, las cuales fueron valoradas, y aquellas que se consideraron procedentes fueron incorporadas al informe, mediante ajustes a su contenido.

SIGLAS

1.24. La descripción de las siglas utilizadas en este documento se detalla a continuación:

SIGLA	**Significado**
CGR	Contraloría General de la República
DFOE	División de Fiscalización Operativa y Evaluativa de la CGR
LGCI	Ley General de Control Interno
NTCGTI	Normas Técnicas para el Control y Gestión de las Tecnologías de Información
NGASP	Normas Generales de Auditoría para el Sector Público
MAGEFI	Manual General de Fiscalización Integral
SINIRUBE	Sistema
ISO	Organización Internacional para la Estandarización, por sus siglas en inglés
COBIT	Objetivos de Control para Información y Tecnologías Relacionadas
BAI	Construir, Adquirir e Implementar por sus siglas en inglés.
DSS	Entregar, dar servicio y soporte en sus siglas en inglés
APO	Alinear, Planificar y Organizar por sus siglas en inglés

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2. Resultados

2.1. El estudio considera tres áreas temáticas, a saber: seguridad de la información, operaciones (incluye la gestión de carga de datos) y procesos de TI, que contempla actividades propias de gestión de servicios y funcionalidad del sistema. A continuación se detallan las oportunidades de mejora más relevantes que se encuentran como resultado del examen de los principales controles relacionados con funcionalidad y operaciones.

2.2. En la redacción de los resultados, cuando se refiere a "usuarios del sistema" se entenderá como los funcionarios de las instituciones que interactúan con el SINIRUBE.

FUNCIONALIDAD DEL SISTEMA (CARGA DE DATOS)

2.3. *La funcionalidad se refiere a la capacidad que tiene un sistema para realizar correcta y completamente las tareas para las cuales fue diseñado, atendiendo las necesidades y criterio de los usuarios. Donde se contempla además, el proceso de actualización periódica de datos provenientes de las diferentes fuentes institucionales, el cual es fundamental para la actualización de la información.*

Seguimiento y actualización de información en el sistema

2.4. Un 95% (75/79) de las instituciones usuarias del sistema no remiten con la frecuencia convenida al SINIRUBE la información requerida para actualizar la base de datos. Además, se visualizan casos en que el personal del SINIRUBE, encargado de actualizar la información proveniente de las instituciones, se atrasa en la carga de información; de manera que el sistema no se actualiza con la prontitud debida. En esa misma línea, un 32,1% (68/211) de los usuarios perciben que el sistema no cuenta con información actualizada y ajustada a la realidad.

2.5. En septiembre de 2020, la Administración realizó una encuesta de satisfacción general (9 preguntas) sobre el aplicativo web, enfocada a temas relacionados con la frecuencia de uso y la atención de consultas y de acuerdo con lo informado, los encuestados manifestaron inquietudes con respecto a la actualización de los datos.

2.6. Importante acotar que el sistema fue creado desde el año 2013, mediante la Ley N.° 9137[1] como herramienta al servicio de otras instituciones públicas y que no existe de forma aislada o para ser un sistema transaccional, sino más bien como medio de consulta, único y centralizado que debe servir como base para la toma de decisiones.

2.7. En este sentido, uno de los aspectos clave es la calidad de la información, para lo cual los datos deben cumplir criterios de oportunidad y pertinencia. Ambos factores aunados a la utilidad y calidad contextual entre otros, apoyan la evaluación de la situación económica y social de los aspirantes a beneficios sociales por parte del Estado y propician correcta distribución de los fondos que las instituciones públicas destinan para el auxilio de poblaciones vulnerables (niños, ancianos, desempleados, personas sin una solución habitacional, etc.)

[1] Emitida el 30 de abril de 2013 y publicada en la Gaceta 170' del 5 de septiembre de 2013.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.8. Dichos aspectos son tomados en cuenta por la Ley General de Control Interno N.° 8292[2]. que en el artículo 8 indica, entre otras cosas, que se debe garantizar la "confiabilidad y oportunidad de la información" y "garantizar la eficiencia y eficacia de las operaciones".

2.9. Análogamente, las Normas de Control Interno para el Sector Público N-2-2009-CO-DFOE[3] en su artículo 16, establecen que los sistemas de información deben contar con procesos que permitan identificar y registrar información confiable, relevante, pertinente y oportuna. Además, señala que la información debe ser comunicada a la administración activa que la necesite, en la forma y dentro del plazo requerido para el cumplimiento adecuado de sus responsabilidades, incluidas las de control interno.

2.10. De igual forma las Normas Técnicas para la gestión y el control de las Tecnologías de Información emitidas por la CGR (NTCGTI)[4] establecen, en el inciso "e" del aparte sobre Administración y operación de la plataforma tecnológica, que se deberá "controlar la ejecución de los trabajos mediante su programación, supervisión y registro."

2.11. A su vez, el Cobit 5 (ISACA 2012) indica en su proceso APO11 "Gestionar la Calidad", en la práctica de gestión 01, que se debe "establecer un sistema de gestión de la calidad (…) que proporcione una aproximación a la gestión de la calidad para la información, la tecnología y los procesos de negocio que sea continua, estandarizada, formal y que esté alineada con los requerimientos del negocio y con la gestión de la calidad a nivel corporativo". Por su parte, el proceso DSS01 tiene como meta "las actividades operativas se realizan según lo requerido y programado" así como asegurar que "Las operaciones son monitorizadas, medidas, reportadas y remediadas" y en ese sentido la práctica 1 sobre procedimientos operativos indica a nivel de actividad que se debe "verificar que todos los datos esperados para su procesamiento sean recibidos y procesados por completo y de una forma precisa y oportuna. Entregar los resultados de acuerdo con los requisitos de la empresa. Dar soporte a las necesidades de reinicio y reprocesamiento. Asegurar que los usuarios reciben los resultados adecuados de una forma segura y oportuna."

2.12. Sobre el particular, para la carga de datos SIVAR el sistema posee un seguimiento de las cargas efectivas y no efectivas, así como de los errores detectados, al remitir un correo automático al usuario. No obstante, el SINIRUBE no ha diseñado una estrategia de seguimiento periódico y sistematizado a las instituciones para garantizar la entrega oportuna de la información y actualización de datos para las cargas recibidas por medio del protocolo FTP.

2.13. Lo comentado evidencia la posibilidad de datos desactualizados para las cargas recibidas por medio del protocolo FTP, así como un riesgo de pérdida de integridad de la información, lo cual puede repercutir en la toma de decisiones por parte del usuario final.

PROCESOS DE TI

2.14. Los procesos de TI son la guía que considera todas aquellas actividades dentro de la unidad administrativa encargada de las tecnologías de información que se ejecutan para el cumplimiento de los objetivos de la institución.

[2] Emitida el 31 de julio de 2002 y publicada en la Gaceta 69 del 4 de septiembre de 2002.

[3] Emitidas el 26 de enero de 2009. , publicadas en la Gaceta Nº 26 del 6 de febrero de 2009.

[4] N.° R CO 26 2007 del 7 de junio de 2007, publicadas en la Gaceta N.° 119 del 21 de junio de 2007.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Gestión de Riesgos

2.15. El SINIRUBE como ente desconcentrado, no ha implementado el proceso de valoración de riesgos en materia de tecnologías de información y procesos de negocio, siendo que únicamente la institución cuenta con una valoración externa realizada por una empresa consultora en el año 2019, para el apoyo del proceso de planificación estratégica y operativa, sin que se haya establecido dicho proceso de manera formal para su ejecución periódica, como parte del sistema de control interno institucional.

2.16. Sobre el particular, el artículo 10 la Ley de General de Control Interno N.° 8292 (LGCI)[5] indica que serán responsabilidad del jerarca y de los titulares subordinados establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional, así como realizar las acciones necesarias para garantizar su efectivo funcionamiento.

2.17. En el tema particular de riesgos la citada ley en su artículo 14 señala además, que como parte de sus responsabilidades el jerarca y los titulares subordinados deben identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, el efecto posible de los riesgos identificados, su importancia y la probabilidad de que ocurran; adoptar las medidas necesarias para el funcionamiento adecuado del sistema de valoración del riesgo y para ubicarse por lo menos en un nivel de riesgo organizacional aceptable; así como establecer los mecanismos operativos que minimicen el riesgo en las acciones por ejecutar.

2.18. En ese sentido, las Normas Técnicas para la gestión y el control de las Tecnologías de Información emitidas por la CGR[6] (NTCGTI), en su inciso 1.3) Gestión de riesgos, señalan que "la organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable."

2.19. Además, Cobit 5 (ISACA 2012) en el proceso APO12 sobre la Gestión del Riesgo señala que este consiste en "identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa." En este proceso se tienen prácticas de gestión relacionadas con recopilar datos (APO12.01) "Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.", analizar el riesgo (APO12.02) "Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo.", y mantener un perfil de riesgo (APO12.03) "Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados.".

2.20. A su vez, en la ISO IEC 27001:2014, Técnicas de seguridad - Sistemas de gestión de la seguridad de la información, en el aparte 6 de planificación, inciso 6.1 Acciones para abordar los riesgos y las oportunidades, se señala que "La organización debe planificar: d) las acciones para hacer frente a estos riesgos y oportunidades, y e) la forma de 1) integrar e implementar las acciones dentro de los procesos de su sistema de gestión de seguridad de la información, y 2) evaluar la eficacia de estas acciones.". Además, con respecto a la valoración

[5] Emitida el 18 de julio de 2002 y publicada Gaceta N.° 169 del 4 de septiembre de 2002.

[6] N.° R CO 26 2007 del 7 de junio de 2007, publicadas en la Gaceta N.° 119 del 21 de junio de 2007.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

del riesgo de seguridad de la información (6.1.2), se establece que " La organización debe definir y aplicar un proceso de valoración del riesgo de seguridad de la información que: a) establezca y mantenga los criterios de riesgo de seguridad de la información que incluyan: 1) los criterios de aceptación del riesgo, y 2) los criterios para realizar las valoraciones del riesgo de seguridad de la información; b) asegure que las valoraciones del riesgo de seguridad de la información repetidas produzcan resultados coherentes, válidos y comparables. c) identifique los riesgos de seguridad de la información., d) analice el riesgo de seguridad de la información, e) evalúe los riesgos de seguridad de la información".

2.21. La carencia del procedimiento de gestión de riesgos dentro del SINIRUBE como órgano de desconcentración máxima se debe a que este proceso ha venido siendo únicamente un insumo para la gestión de riesgos del IMAS y no se ha desarrollado esta gestión para apoyar la toma de decisiones del SINIRUBE como órgano independiente.

2.22. La ausencia de una valoración de riesgo de TI y de los procesos del negocio, provoca que las actividades relacionadas no se prioricen tomando en cuenta estos elementos y que se pueda generar una afectación sobre la organización al no realizar una adecuada canalización de sus recursos hacia las actividades de mayor riesgo.

Procesos de Gestión de Mesa de Ayuda y Gestión de Incidentes

2.23. El SINIRUBE no ha establecido de manera formal un punto de contacto único (conocido como mesa de ayuda) para atender los requerimientos del usuario final y más bien, utiliza herramientas de software de uso interno para el registro manual y control de los requerimientos del usuario. Según manifestaciones de los usuarios, no se ha desarrollado una plataforma de gestión de requerimientos e incidentes y se comprobó que, a pesar de que existen números de teléfonos y correos electrónicos que los usuarios podrían utilizar, esa información no es comunicada por el SINIRUBE y por tanto los usuarios desconocen estos mecanismos.

2.24. Asimismo, con respecto a la atención de consultas y problemas de los usuarios, un 74,5% (146/196) de éstos no tiene un conocimiento claro sobre el tema. En cuanto a la capacitación brindada por la Administración un 75,2% (147/196) señala que la recibió hace más de un año y un 85,2% (167/196) indica que no recibió una guía o manual para consultar en caso de que fuese necesario.

2.25. En la planificación de tecnologías de información (TI), la administración cuenta con un proyecto relacionado con la consolidación y actualización de la mesa de servicios, el cual, en un principio, fue programado para el año 2020, sin embargo SINIRUBE no lo logró ejecutar. Según consta en el estado de los proyectos remitido por la administración, este se reprogramó para los años 2021 y 2022, y se espera que el proceso de licitación/contratación esté incorporado en SICOP al primer semestre 2021.

2.26. En esa línea, las Normas Técnicas para la gestión y el control de las Tecnologías de Información emitidas por la CGR (NTCGTI)[7] establecen en el inciso 1.4.7) Continuidad de los servicios de TI, que "la organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios." Por su parte el inciso 1.2), establece que "la organización debe generar los productos y servicios de TI de

[7] N.° R CO 26 2007 del 7 de junio de 2007, publicadas en la Gaceta N.° 119 del 21 de junio de 2007

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

conformidad con los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo".

2.27. A su vez, el Cobit 5 (ISACA 2012) en la práctica de gestión APO11.03 (Enfocar la gestión de la calidad en los clientes) indica que se debe "enfocar la gestión de la calidad en los clientes, mediante la **determinación de sus necesidades** y asegurar el alineamiento con las prácticas de gestión de calidad" (el destacado no es del original).

2.28. En el capítulo IV Prestación de Servicios, aparte 4.4) "Atención de requerimientos de los usuarios de TI. La organización debe hacerle fácil al usuario el proceso para solicitar la atención de los requerimientos que le surjan al utilizar las TI. Asimismo, debe atender tales requerimientos de manera eficaz, eficiente y oportuna; y dicha atención debe constituir un mecanismo de aprendizaje que permita minimizar los costos asociados y la recurrencia; 4.5) Manejo de incidentes La organización debe identificar, analizar y resolver de manera oportuna los problemas, errores e incidentes significativos que se susciten con las TI. Además, debe darles el seguimiento pertinente, minimizar el riesgo de recurrencia y procurar el aprendizaje necesario; 4.6) Administración de servicios prestados por terceros. La organización debe asegurar que los servicios contratados a terceros satisfagan los requerimientos en forma eficiente. Con ese fin, debe:

a) Establecer los roles y responsabilidades de terceros que le brinden servicios de TI.

b) Establecer y documentar los procedimientos asociados con los servicios e instalaciones contratadas a terceros.

c) Vigilar que los servicios contratados sean congruentes con las políticas relativas a calidad, seguridad y seguimiento establecidas por la organización.

d) Minimizar la dependencia de la organización respecto de los servicios contratados a un tercero.

e) Asignar a un responsable con las competencias necesarias que evalúe periódicamente la calidad y cumplimiento oportuno de los servicios contratados."

2.29. A su vez, la ISO IEC 27001:2014, Técnicas de seguridad - Sistemas de gestión de la seguridad de la información, aparte 16) "Gestión de incidentes de seguridad de la información", inciso 16.1 "Gestión de incidentes y mejoras en la seguridad de la información", establece que dicha gestión tiene como objetivo "Asegurar que se aplique un enfoque coherente y efectivo para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación de los eventos y debilidades de seguridad"; inciso 16.1.1 "Responsabilidades y procedimientos." Se señala que "deben establecer responsabilidades y procedimientos de gestión para asegurarse de tener una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información"; inciso 16.1.2 "Reporte de eventos de seguridad de la información. Los eventos de seguridad de la información deben ser reportados a través de canales de gestión adecuados tan pronto como sea posible".

2.30. En el inciso 16.1.3 "Reporte de debilidades de seguridad de la información. Los empleados y contratistas que utilizan los sistemas y servicios de información de la organización deben estar obligados a notar y reportar cualquier debilidad observada o sospechosa de la seguridad de la información en los sistemas o servicios."; inciso 16.1.4. "Evaluación y decisión sobre los eventos de seguridad de la información. Los eventos de seguridad de la información deben ser evaluados y se debe decidir si serán clasificados como incidentes de seguridad de la

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

información.”; inciso 16.1.5 “Respuesta a incidentes de seguridad de la información. Se deben responder los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.”; inciso 16.1.6. “Aprendiendo de los incidentes de seguridad información. El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe ser utilizado para reducir la posibilidad o el impacto de incidentes en el futuro.”; inciso 16.1.7. “Recolección de evidencia. La organización debe definir y aplicar procedimientos para la identificación, recopilación, adquisición y preservación de la información, que puede servir como evidencia.”

2.31. Asimismo, el Cobit 5 (ISACA 2012), indica en su proceso DSS02 “Gestionar Peticiones e Incidentes de Servicio. Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.”; DSS02.01 “Definir esquemas de clasificación de incidentes y peticiones de servicio. Definir y comunicar la naturaleza y las características de los potenciales incidentes relacionados con seguridad para que puedan ser fácilmente reconocidos y su impacto entendido y, así, permitir una respuesta adecuada.”; DSS02.02 “Registrar, clasificar y priorizar peticiones e incidentes. Identificar, registrar y clasificar peticiones de servicio e incidentes, y asignar una prioridad según la criticidad del negocio y los acuerdos de servicio.”

2.32. En el DSS02.03 “Verificar, aprobar y resolver peticiones de servicio. Seleccionar los procedimientos adecuados para peticiones y verificar que las peticiones de servicio cumplen los criterios de petición definidos.”; DSS02.04 “Investigar, diagnosticar y localizar incidentes. Identificar y registrar síntomas de incidentes, determinar posibles causas y asignar recursos a su resolución.”; DSS02.05 “Resolver y recuperarse ante incidentes. Documentar, solicitar y probar las soluciones identificadas o temporales y ejecutar acciones de recuperación para restaurar el servicio TI relacionado.”; DSS02.06 “Cerrar peticiones de servicio e incidentes. Verificar la satisfactoria resolución de incidentes y/o satisfactorio cumplimiento de peticiones, y cierre.”

2.33. Como se ha mencionado, esta situación de carencia de una mesa de ayuda en SINIRUBE, se presenta debido a la postergación de los proyectos de consolidación y actualización de los instrumentos para atender las necesidades de los usuarios respecto a la operación del sistema.

2.34. Al respecto, los usuarios del SINIRUBE se podrían enfrentar a problemas relacionados con la gestión de servicios y soporte, como son la omisión de registros de las solicitudes, defectos en su clasificación y priorización, plazos de atención inadecuados y limitado monitoreo y seguimiento.

Procesos de Capacidad de la plataforma tecnológica

2.35. Para satisfacer las necesidades tecnológicas de una organización, tanto actuales como futuras, se deben llevar a cabo mediciones y monitoreo sobre el desempeño adecuado de los equipos y sistemas que están relacionados a las soluciones tecnológicas, esto se conoce como gestión de la capacidad de la plataforma tecnológica.

2.36. En el caso puntual de SINIRUBE, no se ha implementado un proceso periódico de diagnóstico de capacidad de sus equipos y sistemas, a pesar de que la administración acredita la realización de un estudio reciente para conocer la brecha real de lo requerido para el crecimiento de la capacidad del sistema, con el objetivo futuro de asegurar la oportuna y

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

adecuada inversión de recursos en tecnología para garantizar disponibilidad, agilidad y oportunidad de la información que brinda el SINIRUBE a sus usuarios

2.37. En ese sentido, las Normas Técnicas para la gestión y el control de las Tecnologías de Información emitidas por la CGR (NTCGTI)[8] inciso 1.4), establecen que "La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe: b. Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas. c. Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la disponibilidad, obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas."

2.38. Por su parte, el Cobit 5 (ISACA 2012) en su proceso BAI04 sobre la Gestión de la Disponibilidad y la Capacidad, establece que su fin consiste en "Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados.", el cual tiene como una de sus prácticas, el "Evaluar la disponibilidad, el rendimiento y la capacidad de los servicios y recursos para asegurar que se encuentra disponible una capacidad y un rendimiento justificables en costes para dar soporte a las necesidades del negocio y para entregar el servicio de acuerdo a los ANSs."

2.39. Además, dentro de las actividades señala: "1. Considerar en la evaluación (actual o prevista) de disponibilidad, rendimiento y capacidad de servicios y recursos lo siguiente: Requisitos del cliente, prioridades de negocio, objetivos de negocio, impacto en el presupuesto, utilización de recursos, capacidades de TI y tendencias de la industria. 2. Supervisar el rendimiento y la utilización de la capacidad reales frente a los umbrales definidos, con el apoyo cuando sea necesario de software automatizado. 3. Identificar y dar seguimiento a todos los incidentes causados por un rendimiento o una capacidad inadecuados. 4. Evaluar periódicamente los niveles reales de rendimiento a todos los niveles de procesamiento (la demanda del negocio, capacidad de servicio y capacidad de los recursos) mediante la comparación con las tendencias y los ANSs, teniendo en cuenta los cambios en el entorno."

2.40. A su vez, la ISO 27002:2009 Tecnología de la información-Código de prácticas para la gestión de la seguridad de la información, en el aparte 10.3.1 sobre Gestión de la capacidad, señala que "Se debería supervisar y adaptar el uso de recursos, así como proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.", además, establece que las organizaciones "Se debería dar seguimiento y adaptar el sistema para asegurar, y cuando sea necesario, mejorar la disponibilidad y la eficacia de los sistemas. Se debería ejecutar controles exhaustivos para indicar problemas a su debido tiempo. Las proyecciones de los requisitos de capacidad futura deberían tomar en cuenta los nuevos requisitos del negocio y del sistema, así como tendencias actuales y proyectadas en la capacidad de procesamiento de la información de la organización."

2.41. Por tanto, la falta del establecimiento de una periodicidad para gestionar la capacidad de la plataforma tecnológica, no le permite a la administración establecer acciones sobre este tema

[8] N.° R CO 26 2007 del 7 de junio de 2007, publicadas en la Gaceta N.° 119 del 21 de junio de 2007

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

y tomar decisiones para mantener los niveles de calidad y respuesta adecuados del SINIRUBE.

2.42. Al respecto, la Administración señala que el SINIRUBE ha planeado desarrollar una plataforma superior, para sostener el crecimiento del sistema, no obstante, este proyecto no se ha concretado y requiere de un monto presupuestario significativo, el cual es un aspecto incierto, debido a la situación financiera del país.

3. Conclusiones

3.1. El SINIRUBE como sistema, cumple en un sentido amplio, con los objetivos para los cuales fue creado, donde destaca servir como una herramienta que soporta la toma de decisiones operativas, sin embargo, presenta oportunidades de mejora en lo que respecta a su funcionalidad.

3.2. El SINIRUBE, según el criterio de sus usuarios, es una herramienta fácil de utilizar, la mayoría considera que el sistema le proporciona lo requerido para el cumplimiento de sus tareas, no obstante, algunos usuarios perciben que la información no está actualizada, y sufren aspectos relacionados con capacitación y atención de incidentes y consultas sobre la operación del sistema.

3.3. Existen debilidades en el control de la actualización de información que repercuten sobre su procesamiento y utilidad para la toma de decisiones y podrían afectar la oportuna asignación de recursos para mejorar la calidad de vida de los posibles beneficiarios de ayudas del Estado.

3.4. En materia de gestión se presentan oportunidades de mejora en la gestión de la medición del desempeño actual y futuro de su plataforma tecnológica para una adecuada inversión oportuna que garantice la capacidad de los servicios que brinda la institución.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

4. Disposiciones

4.1. De conformidad con las competencias asignadas en los artículos 183 y 184 de la Constitución Política, los artículos 12 y 21 de la Ley Orgánica de la Contraloría General de la República, N.° 7428, y el artículo 12 inciso c) de la Ley General de Control Interno, se emiten las siguientes disposiciones, las cuales son de acatamiento obligatorio y deberán ser cumplidas dentro del plazo (o en el término) conferido para ello, por lo que su incumplimiento no justificado constituye causal de responsabilidad.

4.2. Para la atención de las disposiciones incorporadas en este informe deberán observarse los "Lineamientos generales para el cumplimiento de las disposiciones y recomendaciones emitidas por la Contraloría General de la República en sus informes de auditoría", emitidos mediante resolución N.° R-DC-144-2015, publicados en La Gaceta N.° 242 del 14 de diciembre del 2015, los cuales entraron en vigencia desde el 4 de enero de 2016

4.3. Este órgano contralor se reserva la posibilidad de verificar, por los medios que considere pertinentes, la efectiva implementación de las disposiciones emitidas, así como de valorar el establecimiento de las responsabilidades que correspondan, en caso de incumplimiento injustificado de tales disposiciones.

AL MASTER ERICKSON ÁLVAREZ CALONGE EN SU CALIDAD DE DIRECTOR EJECUTIVO DEL SINIRUBE O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.4. Implementar un mecanismo de control para que la entrega periódica de información por parte de las instituciones se cumpla de acuerdo con lo estipulado en los convenios suscritos; y que contenga al menos la documentación (trazabilidad del control), responsables y actividades relacionadas, con el fin de mantener el flujo y actualización de los datos como una constante en el SINIRUBE (ver párrafos del 2.4 al 2.13). Para acreditar el cumplimiento de esta disposición, deberá remitirse al Órgano Contralor, a más tardar el **14 de setiembre 2021**, una certificación de que dicho mecanismo fue implementado.

4.5. Implementar un mecanismo de control para la recepción y actualización de datos en el sistema desde el punto de vista operacional, que incluya al menos la definición de los medios para identificar, procesar, controlar y evidenciar la recepción y carga de datos individualmente (lotes). (ver párrafos del 2.4 al 2.13) Para acreditar el cumplimiento de esta disposición, deberá remitirse al Órgano Contralor, a más tardar **14 de setiembre 2021**, una certificación de que dicho mecanismo fue implementado.

4.6. Elaborar, divulgar e implementar un procedimiento de gestión de riesgos institucionales y en particular de Tecnologías de Información, acorde a lo estipulado en la Ley de Control Interno, que apoye la toma de decisiones institucional y a sus mecanismos de planificación. (ver párrafos del 2.15 al 2.22) Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor, a más tardar **15 de marzo 2022**, una certificación la cual haga constar que dicho procedimiento se elaboró y oficializó, y a más tardar **15 de abril 2022**, una certificación de que dicho procedimiento fue divulgado e implementado.

4.7. Implementar medidas que garanticen la comunicación con sus usuarios para una correcta atención de incidentes y consultas sobre la operación del sistema. (ver párrafos del 2.23 al

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

2.34). Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor, a más tardar el **15 de noviembre 2021**, una certificación que haga constar que se implementaron las medidas de atención a sus usuarios.

4.8. Implementar el proceso periódico de diagnóstico de capacidad de sus equipos y sistemas, en el cual se analicen las necesidades técnicas, materiales, humanas y de información del SINIRUBE, tanto presentes como proyectadas para sustentar el crecimiento, las inversiones en tecnología, los compromisos adquiridos y el cumplimiento regulatorio (ver párrafos del 2.35 al 2.43). Para dar cumplimiento a esta disposición, a más tardar el **14 de agosto 2021**, se deberá remitir al Órgano Contralor una certificación donde conste la instauración del proceso de medición de capacidad de la tecnología.

Manuel Corrales Umaña
Gerente de Área

Silvia López Villalobos
Asistente Técnico

María José Láscarez Granados
Colaborador

Jonathan Escalante Jiménez
Colaborador

Alejandro Zúñiga Gómez
Coordinador

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica

Anexo N.° 1

Glosario

Término	Concepto
Calidad Contextual	Para el marco de Gobierno y Gestión Cobit 5, se refiere a las propiedades de la información que le hacen útil para ser utilizada en los procesos de TI y de negocio, estas son la precisión, objetividad y el apego a criterios de calidad conocidos.
Gestión de Calidad	Proceso que desarrolla el área de TI para brindar razonabilidad con respecto a las características de la información / datos que ingresan en un sistema, y a lo largo de su ciclo de vida, en función de un conjunto de parámetros o reglas conocidas. Suele asociarse a la integridad de la información entendida como la completitud y la ausencia de errores.
Gestión de Capacidad	Proceso ejecutado por el equipo de gestión (personal de TI) para equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costos. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados.
Gestión de Incidentes	Componente o función de servicio de TI implementado para minimizar el impacto negativo de los incidentes mediante la restauración del funcionamiento normal del servicio lo más rápidamente que sea posible.
Mesa de Ayuda	Se refiere a un conjunto de recursos tecnológicos (incluye sistemas de información) y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados con las Tecnologías de la Información y la Comunicación. También se entiende como el punto de contacto único entre los usuarios y el personal técnico que está a cargo de la solución de incidencias y la atención de requerimientos.

Contraloría General de la República
T: (506) 2501-8000, F: (506) 2501-8100 C: contraloria.general@cgr.go.cr
http://www.cgr.go.cr/ Apdo. 1179-1000, San José, Costa Rica