INFORME NRO. **DFOE-BIS-IF-00002-2021**
27 de mayo, 2021

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

2021

CONTENIDO

P3-04-GE-01 V6

ANEXOS

ANEXO NRO. 1

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 seguridad de información, en específico para determinar si la plataforma actual de SINIRUBE cumple con los principios de seguridad de la información relacionados con la confidencialidad, disponibilidad e integridad del sistema.

¿POR QUÉ ES IMPORTANTE?

La ley de creación del SINIRUBE así como su reglamento, le confiere una serie de obligaciones y responsabilidades a este Órgano, siendo una de las más relevantes el 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 de 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 lo que respecta a la preservación de los principios de confidencialidad, disponibilidad e integridad de la información, se evidenció que el SINIRUBE no cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI). En consecuencia, tampoco ha implementado controles vinculados con la prevención y detección de eventos de seguridad, ni planes de tratamiento del riesgo de seguridad de la información. La ausencia de actividades que desarrollen la estrategia de seguridad en el corto plazo representa un asunto apremiante que se debe atender, especialmente por la sensibilidad de la información contenida en el sistema y la privacidad que debe garantizarse a los beneficiarios, aspectos.

Como parte de la carencia de este SGSI, el SINIRUBE no ha avanzado hacia la elaboración de un Plan de Continuidad del Servicio, que garantice la disponibilidad de la información para la toma de decisiones y su recuperación en caso de que se presenten eventos adversos a su operación. El sistema solo cuenta con prácticas de prevención para eventos puntuales y menores debidos a fallas técnicas en el funcionamiento de los equipos.

Finalmente, se visualizan debilidades en materia de seguridad lógica en cuanto al proceso de gestión de identidades, segregación de funciones de operación de TI incompatibles, supervisión de usuarios con altos privilegios y gestión de contraseñas del sistema SINIRUBE.

¿QUÉ SIGUE?

Con el propósito de fortalecer la gestión de tecnologías de información del SINIRUBE y de garantizar la seguridad de la información, se giran disposiciones a la Dirección Ejecutiva para que se solventen las debilidades en cuanto a continuidad del servicio, seguridad lógica y segregación de funciones incompatibles en la operación del sistema. Lo anterior como controles complementarios hasta que el SINIRUBE cuente con su SGSI implementado de acuerdo con la planeación estratégica de la institución.

INFORME NRO. DFOE-BIS-IF-00002-2021

**DIVISIÓN DE FISCALIZACIÓN OPERATIVA Y EVALUATIVA
ÁREA DE FISCALIZACIÓN PARA EL DESARROLLO
DEL BIENESTAR SOCIAL**

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

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 entre más de 80 instituciones para hacerlo llegar a una población debidamente pre seleccionada es una tarea que requiere de información oportuna y actualizada para tomar decisiones, para orientar correctamente los recursos disponibles, es necesario que se conozca 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.

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 va a aportar 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 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 seguridad de información, en específico para determinar si la plataforma actual de SINIRUBE cumple con los principios de seguridad de la información relacionados con la confidencialidad, disponibilidad e integridad del sistema.

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. Se realizó una visita de campo al Centro de Procesamiento de Datos ubicado en el Mall San Pedro.

1.14. Además, se tuvo acceso al sistema mediante una cuenta temporal para cada miembro del equipo que permitió acceder al sistema a nivel web, 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.

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

ASPECTOS POSITIVOS QUE FAVORECIERON LA EJECUCIÓN DE LA AUDITORÍA

1.16. 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 en temas relacionados con el SINIRUBE.

LIMITACIONES QUE AFECTARON LA EJECUCIÓN DE LA AUDITORÍA

1.17. 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 en el SINIRUBE.

GENERALIDADES ACERCA DEL OBJETO AUDITADO

1.18. 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). Al mismo tiempo, se entiende por SINIRUBE el sistema de información, es decir, el término es dual, se refiere a una organización como conjunto de personas y recursos y a una aplicación desarrollada para su uso a través de Internet.

1.19. 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, 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 pobres de la sociedad.

1.20. 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.

MEJORAS IMPLEMENTADAS POR LA ADMINISTRACIÓN DURANTE LA AUDITORÍA

1.21. En lo que respecta a seguridad física y ambiental, se detectaron oportunidades de mejora, la administración indicó que se encuentra en proceso de contratación de un servicio de arrendamiento para proveer un sitio seguro para sus equipos. A la fecha de cierre de este informe no se tenía certeza del avance de dicha contratación.

1.22. Como parte de este estudio se llevó a cabo un análisis de vulnerabilidades de la plataforma expuesta en Internet, se le entregó a la administración el resultado de dicho análisis y de inmediato se dieron a la tarea de preparar un plan de acción para subsanar dichas debilidades a la brevedad posible. Dado su contenido vulnerable, este informe fue catalogado como confidencial para no exponer debilidades técnicas de la administración a terceros que podrían aprovecharlas para perpetrar ataques.

COMUNICACIÓN PRELIMINAR DE LOS RESULTADOS DE LA AUDITORÍA

1.23. 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.

1.24. 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

1.25. 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

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 contemplan 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 la seguridad de la información.

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

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

2.3. El direccionamiento de la seguridad de la información y la definición de su estrategia son tareas que le competen a los altos mandos en la estructura organizacional. Este marco de seguridad de información debe verse plasmado en un Sistema de Gestión de la Seguridad de la Información que permita gestionar los riesgos y asegurar la confidencialidad, disponibilidad e integridad de los datos que se capturan, procesan y almacenan en los sistemas de información.

2.4. En el caso de SINIRUBE, dada la naturaleza sensible de los datos que son almacenados en sus sistemas de información, se hace aún más crítico contar con buenos controles que garanticen la confidencialidad y buen manejo de la información y la privacidad de los beneficiarios.

2.5. SINIRUBE cuenta con un plan estratégico donde se establece la necesidad de contar con el SGSI a mediano y largo plazo, no obstante, dada la sensibilidad de la información que se almacena en su sistema y la exposición que se presenta al ser información que es consultada y procesada a través de la red Internet, se deben tomar acciones inmediatas en algunos de los campos más críticos de este SGSI, los cuales se enumeran a continuación.

Plan de Continuidad de Servicios de TI y Plan de Recuperación en Caso de Desastre (DRP).

2.6. Un plan de continuidad de servicios de TI garantiza razonablemente la operación de los servicios básicos de TI cuando se presentan situaciones que atentan contra su funcionamiento, gestionando los riesgos y tomando acciones para minimizar su ocurrencia e impacto. Además, una parte importante de este plan lo constituye el plan de recuperación de desastres, que tiene que ser activado cuando un evento adverso se presenta y disminuye la capacidad de entrega de servicios de TI, este plan contiene acciones para el restablecimiento del servicio a los niveles normales de atención.

2.7. La priorización de los servicios que deben restablecerse primero y su nivel mínimo de funcionamiento es establecido a través de un Análisis de Impacto al Negocio (BIA) que es un estudio necesario para poder desarrollar los planes de continuidad de servicio.

2.8. En la actualidad, el sistema SINIRUBE cuenta con configuraciones de redundancia en sus servidores que garantizan de manera razonable gestionar fallos técnicos que podrían presentarse, de manera puntual, en algunos de sus componentes, además, se cuenta con respaldos periódicos de información y un procedimiento para la restauración de estos.

2.9. No obstante lo anterior, SINIRUBE no cuenta con una estrategia de Continuidad de Servicios que establezca los planes necesarios para garantizar la disponibilidad de la información relevante en caso de fallas o eventos mayores que atenten contra el funcionamiento de sus sistemas, sean estos provocados por eventos naturales, fallas mayores e inclusive acción delictiva.

2.10. En esta línea, las buenas prácticas de redundancia de dispositivos y de respaldo, implementadas por SINIRUBE, no responden a una estrategia integrada y resultan útiles únicamente para resolver fallas menores. Además, no se tienen procedimientos que verifiquen el estado de los respaldos para su eventual uso en caso de ser requeridos.

2.11. Algunos de los riesgos de continuidad, que están latentes en SINIRUBE pudieron observarse como resultado de la visita de campo efectuada a su centro de datos, donde se observó que su sala de servidores presenta debilidades en la protección contra incendio, pues no existen sistemas supresores de fuego y en cuanto al acondicionamiento de la temperatura, este se lleva a cabo por medio de un único equipo de aire acondicionado, el cual se presenta como un punto de falla sin redundancia, situaciones que deberían ser parte de los planes de continuidad.

2.12. Lo descrito en los párrafos anteriores no es congruente con lo establecido en las Normas de Control Interno para el Sector Público (NCISP)[1], las cuales, en el aparte 5.9, estipulan que "deben instaurarse los mecanismos y procedimientos manuales que permitan garantizar razonablemente la operación continua y correcta de los sistemas de información".

2.13. Por su parte, las Normas Técnicas para la gestión y el control de las Tecnologías de Información de la CGR (NTGCTI)[2], en el inciso 1.4) establecen que "la organización debe garantizar, de manera razonable, la **confidencialidad, integridad y disponibilidad** de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales. Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos: (…) La **continuidad de los servicios de TI**" (el destacado no es del original).

2.14. Adicionalmente, el inciso 1.4.7) indica que "la organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios. Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad".

2.15. Por otra parte, Cobit 5 (ISACA 2012), en su proceso DSS04 "Gestionar la Continuidad" indican que se debe "**establecer y mantener un plan** para permitir al negocio y a TI **responder a incidentes e interrupciones de servicio** para la operación continua de los

---

[1] Emitidas el 26 de enero de 2009, N-2-2009-CO-DFOE, publicadas en La Gaceta Nº 26 del 6 de febrero de 2009.

[2] Emitidas mediante Resolución Nro. R CO 26 2007 del 7 de junio de 2007 y publicadas en la Gaceta Nro. 119 del 21 de junio de 2007

procesos críticos para el negocio y los servicios TI requeridos y **mantener la disponibilidad** de la información a un nivel aceptable para la empresa" (el destacado no es del original).

2.16. También, la práctica de gestión DSS04.02 "Mantener una estrategia de continuidad" amplía que este proceso implica "evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor o disrupción".

2.17. Así mismo en la práctica de gestión DSS04.03 "Desarrollar e implementar una respuesta a la continuidad del negocio", especifica que este plan debe estar basado en una estrategia que documente los procedimientos y la información requerida para el uso durante y después de un incidente, para facilitar que la empresa continúe con sus actividades críticas.

2.18. En lo que respecta al respaldo y recuperación de información las NTGCTI indican, en su punto 4.2) sobre Administración de la operación de la plataforma tecnológica, inciso h), la necesidad de "definir formalmente y efectuar rutinas de respaldo, custodiar los medios de respaldo en ambientes adecuados, controlar el acceso a dichos medios y establecer procedimientos de control para los procesos de restauración".

2.19. Por su parte, las buenas prácticas establecidas en la ISO 27002:2009 Tecnología de la información-Código de prácticas para la gestión de la seguridad de la información, en su aparte 10.5.1 Respaldos de información, indican que se debería considerar "a) se debería definir el nivel necesario de información de respaldo; b) se debería producir procedimientos documentados de restauración y registros exactos y completos de las copias de respaldo, f) los medios de respaldo se deberían probar regularmente para asegurarse que pueden ser confiables para el uso cuando ser necesarios, g) los procedimientos de restauración deberían ser comprobados regularmente para asegurar que son eficaces y que pueden ser utilizados dentro del tiempo asignado en los procedimientos operacionales para la recuperación."

2.20. De acuerdo con lo manifestado por SINIRUBE, estos planes no existen porque no se ha realizado un análisis del impacto que pueda tener la suspensión de sus sistemas en la prestación de sus servicios, este análisis es básico para orientar la priorización de los esfuerzos de mitigación, basada en riesgos, que considere, además, las consecuencias e impacto de pérdida de información sensible y vital para cumplir con los mandatos que le establece la Ley de brindar un servicio oportuno para favorecer a la población en condición de riesgo del país.

2.21. Además, la estrategia de continuidad de servicios y recuperación de desastres no fue considerada en el diseño inicial de la estrategia de seguridad de información y no se incluyó como parte de los complementos a la Política de Seguridad de Información, en buena medida, debido a que no se ha iniciado la integración de los esfuerzos realizados en materia de seguridad por medio del diseño e implementación de un Sistema de Gestión de Seguridad de Información (SGSI) que es el instrumento administrativo que permite unificar el gobierno de la seguridad.

2.22. La carencia de estas herramientas, vitales para atender eventos adversos, expone al sistema y a la información sensible, contenida en el mismo, a riesgos de pérdida de confidencialidad y privacidad de los datos de la población, así como a la suspensión de los servicios que presta SINIRUBE a otras instituciones, suspensiones que podrían prolongarse por períodos de tiempo que resultarían críticos para la correcta toma de decisiones para asignar beneficios sociales.

Proceso de gestión de privilegios de usuarios del sistema.

2.23. En el campo de la seguridad lógica, las organizaciones deben contar con controles que limiten los accesos, tanto de funcionarios, como de clientes y terceros contratados, a la información de la institución, principalmente a aquella información sensible que debe ser protegida.

2.24. Los buenos controles de acceso lógico deben garantizar que los individuos solamente puedan acceder a la información que es estrictamente necesaria para desempeñar sus funciones y que estos privilegios sean monitoreados para que se ajusten a la realidad institucional en todo momento y se garantice que no se presenten abusos en el uso de la información.

2.25. Este estudio ha revelado que el SINIRUBE no cuenta con procedimientos y regulaciones que se puedan aplicar, de forma inmediata, cuando un usuario cambia de funciones, es suspendido o ya no debe tener acceso al sistema de información, así mismo, no se tienen controles que limiten y verifiquen el uso de usuarios temporales y de usuarios con concentración de altos privilegios de acceso a la información.

2.26. Además, el SINIRUBE no ejerce funciones de monitoreo en el uso del sistema por parte de los usuarios, y en el caso específico de aquellos con altos privilegios, quienes forman parte del equipo de tecnologías de información, solamente se lleva el registro de las consultas en las bitácoras del sistema, las cuales no son revisadas y tampoco incluyen los registros sobre inserciones y borrados, ni se encuentran aisladas del acceso y manipulación por parte de los usuarios con este tipo de privilegio.

2.27. La necesidad de controlar el acceso a la información institucional está normada en la Ley General de Control Interno N.° 8292, publicada en la Gaceta oficial N.° 169 del 4 de setiembre de 2002, donde se establece, en su Artículo 15 sobre Actividades de control, que es responsabilidad del jerarca y titulares subordinados “a) Documentar, mantener actualizados y divulgar internamente, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones.”

2.28. Adicionalmente, en las NTGCTI, punto 1.4.5) Control de Acceso, se señala que la organización debe “f. Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.”

2.29. Por su parte, las buenas prácticas establecidas en el COBIT 5 establecen, en el proceso DSS05.04 sobre Gestión de la identidad del usuario y el acceso lógico, que la organización debe “administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados.”.

2.30. Además, en la proceso DSS06.03 sobre "Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización", de esas mismas buenas prácticas, se indica que se deben "asignar derechos de acceso y privilegios sólo sobre lo que es necesario para ejecutar las actividades de trabajo, basados en los roles de puesto predefinidos. Eliminar o revisar los derechos de acceso inmediatamente si el rol del puesto cambia o un miembro del personal deja el área de proceso de negocio. Revisar periódicamente para asegurar que el acceso es adecuado para las actuales amenazas, riesgos, tecnología y necesidades del negocio."

2.31. En el caso de SINIRUBE, se han omitido los controles que garanticen la correcta asignación y remoción de permisos a sus usuarios con la inmediatez requerida, dada la sensibilidad de la información almacenada en su sistema de información, así mismo, se han omitido controles que monitoreen la actividad de los usuarios, principalmente aquellos funcionarios que cuentan con privilegios altos y que en su mayoría son necesarios para dar el correcto mantenimiento a los sistemas, pero que al tener acceso a toda la información por sus funciones, deben ser supervisados para evitar acciones no deseadas como pueden ser destrucción o fuga de información sensible.

2.32. Un efectivo proceso de control de identidades de los usuarios previene accesos no autorizados a la información que podrían desencadenar pérdidas de confidencialidad e integridad de la información.

2.33. En reunión efectuada con la administración, se acepta la debilidad mencionada e indican que se tomarán las acciones necesarias para el tratamiento de estos riesgos.

Identificación y autenticación de usuarios.

2.34. El proceso de identificación y autenticación de usuarios a un sistema es la primera barrera de seguridad lógica existente. Durante este proceso, el sistema garantiza que la persona que está ingresando cuenta con un acceso debidamente autorizado y que se está acreditando de forma correcta su identidad.

2.35. El proceso de identificación consiste en brindar una identidad diferente y única a cada usuario para poder llevar trazabilidad de sus acciones, y la autenticación de los usuarios consiste en validar que la persona que está intentando acceder a los sistemas es quien dice ser, esto generalmente se lleva a cabo mediante factores de autenticación que pueden ser de tres tipos: algo que solamente el usuario conoce, como una contraseña; algo que solo el usuario posee, como una tarjeta inteligente o un mensaje enviado a su correo electrónico, entre otros; o algo que identifica de manera física (biométrica) al usuario, como su huella digital o reconocimiento facial, entre otros. Los mejores sistemas de autenticación combinan dos o más factores de los descritos anteriormente.

2.36. Cuando un sistema basa la autenticación de sus usuarios en contraseñas, se debe procurar que estas sean robustas, es decir, que cumplan con buenas prácticas para su construcción y que sean cambiadas de manera regular. Dentro de estas buenas prácticas está el uso de una combinación de números, letras y otros símbolos, una longitud mínima determinada, la no reutilización de contraseñas, que estas no contengan nombres, palabras o fechas que puedan ser sujetas de fácil acierto por los atacantes, entre otros parámetros recomendados.

2.37. En el caso del SINIRUBE, en este estudio se determinó que los sistemas automatizados no contemplan el control de la construcción de contraseñas para garantizar razonablemente su fortaleza contra posibles ataques que intenten suplantar la identidad de sus usuarios, asimismo, no se inhibe la reutilización de contraseñas y no se solicita de manera obligatoria el cambio de la contraseña temporal que se le asigna al usuario para su primer ingreso.

2.38. De igual forma, se determinó que los sistemas no bloquean a los usuarios por inactividad de sus equipos, es decir, si un usuario deja desatendido su equipo, luego de un tiempo prudencial, este debería bloquearse y volver a solicitar la autenticación para garantizar que personas no autorizadas no hagan accesos indebidos al sistema.

2.39. La situación descrita en los párrafos anteriores se presenta aun cuando existe una Política de contraseñas en el SINIRUBE (PI-SINIRUBE-012), aprobada en la sesión del Consejo Rector N°09-E-2019, Acuerdo N° 141-2019 del 25 de octubre de 2019, la cual, en el aparte VIII Disposiciones generales de la política, establece lineamientos para establecer contraseñas seguras como lo son: “a.Todas las claves de acceso definidas por defecto por el fabricante en dispositivos de red, servidores, entre otros, deben de ser cambiadas antes de su implementación final en producción, b. Las contraseñas no se deben escribir en ningún lugar. De hacerlo, deberán estar bajo llave en una caja fuerte, dejando el registro correspondiente con la justificación de la necesidad de guardarla escrita. c. Las contraseñas temporales, deben ser modificadas la primera vez que el usuario ingrese al sistema. d. Las contraseñas nunca se deben incluir en mensajes de correo electrónico u otra forma de comunicación electrónica sin cifrar. e.Las contraseñas deberán tener un mínimo de 8 caracteres alfanuméricos no consecutivos, y deberá ser fácil de recordar, pero difícil de adivinar (no deben estar relacionadas con el nombre de usuario, nombres propios, nombres de empresa, fechas de nacimiento). f. Las contraseñas deben tener al menos 2 de las 4 siguientes características: letras mayúsculas, letras minúsculas, números y símbolo. g. Las contraseñas deben cambiarse cada 90 días. h. Cuando se hace un cambio de contraseña, la misma no puede ser igual a las últimas 2 contraseñas. i. No habilitar el recordatorio de contraseñas en los navegadores o páginas de Internet. j. En todos los casos donde aplique se debe limitar a 3 el número de intentos fallidos consecutivos para digitar la contraseña En todos los casos donde aplique se debe limitar a 3 el número de intentos fallidos consecutivos para digitar la contraseña. k. Cuando un usuario requiera solicitar nuevamente su contraseña, ya sea porque su cuenta ha sido bloqueada o porque se le olvidó la contraseña, la cuenta debe ser desbloqueada por el Equipo Técnico del SINIRUBE.”

2.40. Por su parte, NTGCTI, en su punto 1.4) indican que “la organización debe garantizar, de manera razonable, la confidencialidad, e integridad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados.”

2.41. También puntualiza este marco normativo, en su aparte 1.4.5), que “la organización debe proteger la información de accesos no autorizados. Para dicho propósito debe: a. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación. (…), d. Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI, e. Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización y f. Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI.”

2.42. Por su parte, las mejores prácticas incluidas en COBIT 5 incluyen, en el proceso DSS05 "Gestionar los Servicios de Seguridad", la necesidad de "proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad". Este proceso especifica que se deben llevar a cabo, entre otras, las siguientes actividades: "mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. Alinear la gestión de identidades y derechos de acceso a los roles y responsabilidades definidos, basándose en los principios de menor privilegio, necesidad de tener y necesidad de conocer. Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno basándose sólo en transacciones aprobadas y documentadas y autorizadas por los gestores individuales designados".

2.43. Como parte de la ausencia del SGSI, la administración no ha establecido los procesos que operacionalicen el control de la construcción y uso correcto de contraseñas ni los controles para que las políticas en este sentido sean acatadas por el personal técnico que administra los sistemas.

2.44. Como se ha mencionado, un mal uso y un control deficiente en la construcción de contraseñas puede exponer a la institución a un mal manejo y violación de la confidencialidad de la información altamente sensible que se encuentra almacenada en sus bases de datos con repercusiones muy negativas para la institución y la privacidad de los beneficiarios.

Segregación de funciones.

2.45. El personal de Tecnologías de Información de SINIRUBE que lleva a cabo la operación de los equipos y actualización de la información que se recibe de parte de todas las instituciones que forman parte de los convenios de SINIRUBE, no cuenta con una adecuada segregación de funciones críticas, que podrían resultar incompatibles, en el manejo de esta información, como por ejemplo la recepción, autorización y aplicación de los datos que se cargan al sistema, la modificación de parámetros, mantenimiento de la base de datos, entre otras. Además, sus perfiles de privilegios de acceso son excesivos y no obedecen a los principios mencionados de mínimo privilegio.

2.46. Esta situación discrepa de lo establecido en las NCISP que señalan, en el aparte sobre estructura organizativa, la necesidad de autorización, aprobación y de separación de funciones incompatibles así como la rotación de labores. Asimismo, en la sección 2.5.2 indican que "la ejecución de los procesos, operaciones y transacciones institucionales debe contar con la autorización y la aprobación respectivas de parte de los funcionarios con potestad para concederlas, que sean necesarias a la luz de los riesgos inherentes, los requerimientos normativos y las disposiciones institucionales.

2.47. También, en el aparte 2.5.3 señalan que "el jerarca y los titulares subordinados, según sus competencias, deben asegurarse de que las funciones incompatibles, se separen y distribuyan entre los diferentes puestos; así también, que las fases de autorización, aprobación, ejecución y registro de una transacción, y la custodia de activos, estén distribuidas entre las unidades de la institución, de modo tal que una sola persona o unidad no tenga el control por la totalidad de ese conjunto de labores." Además, a falta de segregación por cualquier situación excepcional "deben implantarse los controles alternativos que aseguren razonablemente el adecuado desempeño de los responsables".

2.48. Adicionalmente, este mismo cuerpo normativo, en lo referente al control de rotación de labores, indica que "el jerarca y los titulares subordinados, según sus competencias deben procurar la rotación sistemática de las labores entre quienes realizan tareas o funciones afines, siempre y cuando la naturaleza de tales labores permita aplicar esa medida."

2.49. En esa misma línea las NTGCTI indican, en relación con los controles de acceso, que "el jerarca y los titulares subordinados, según sus competencias, deben procurar la rotación sistemática de las labores entre quienes realizan tareas o funciones afines, siempre y cuando la naturaleza de tales labores permita aplicar esa medida."

2.50. Las debilidades en materia de segregación de funciones se atribuyen a las limitaciones propias de la estructura organizacional de SINIRUBE, ya que no se cuenta con el personal suficiente o en su defecto las horas-hombre necesarias para atender esa separación funcional, y no se han implementado controles complementarios para subsanar esta debilidad.

2.51. Las debilidades en segregación de funciones exponen a la institución a un riesgo de pérdida de confidencialidad y de integridad de la información sensible y crítica de la institución y de otras instituciones, así como la exposición de la privacidad de los beneficiarios, con el agravante de la imposibilidad de establecer responsabilidades.

3. Conclusiones

3.1. En materia de seguridad de información se han dado pasos importantes y se tienen proyectos en curso, algunos de los cuales están priorizados pero sin considerar los riesgos asociados, por lo que algunos asuntos críticos como la continuidad del servicio y el desarrollo de un Sistema de Gestión de la Seguridad de Información están pendientes en términos de diseño y ejecución.

3.2. Existe una exposición a riesgos relevantes en materia de seguridad de información, por cuanto algunos controles críticos, como por ejemplo, la parametrización de contraseñas, la gestión de identidades y la supervisión de usuarios con altos privilegios, merecen una valoración y ajustes para favorecer la confidencialidad, disponibilidad e integridad de la información.

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, Nro. 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 Nro. R-DC-144-2015, publicados en La Gaceta Nro. 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. Establecer el proceso periódico de Análisis de Impacto al Negocio (BIA) de sus procesos críticos, que guíe la definición de planes de continuidad y recuperación de desastres de Tecnologías de Información y sistemas críticos. Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor, a más tardar **14 de septiembre 2021** una certificación en la que se haga constar que dicho proceso de Análisis de Impacto de Negocio (BIA) fue debidamente establecido y elaborado en su primera versión. (Ver párrafos del 2.6 al 2.22)

4.5. Elaborar, someter a aprobación del Consejo Rector y divulgar un Plan de Continuidad de Servicios de TI que incluya un Plan de Recuperación en caso de Desastres (DRP) que consideren los requerimientos mínimos señalados en las buenas prácticas, además de la asignación de roles y responsabilidades. Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor, a más tardar el **14 de enero 2022** una certificación en la cual se haga constar que dicho plan fue debidamente elaborado y remitido al Consejo Rector, y al **14 de enero 2022** una certificación donde conste su divulgación.(Ver párrafos del 2.6 al 2.22)

4.6. Elaborar, divulgar e implementar un procedimiento de gestión de identidades (acceso lógico y control de accesos) y monitoreo de usuarios con altos privilegios, con el fin de que se contemplen las actividades relacionadas con el procesamiento de permutas, suspensiones, administración de usuarios temporales y con altos privilegios. Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor a más tardar **15 de noviembre 2021**, una certificación que haga constar que dicho procedimiento fue definido y oficializado. Además, se deberá remitir a más tardar el **14 de enero 2022** una certificación de que dicho procedimiento fue debidamente divulgado e implementado. (Ver párrafos del 2.23 al 2.33)

4.7. Valorar una modificación de la "Política de contraseñas PI-SINIRUBE-012" vigente y someterla a aprobación del Consejo Rector, con el fin de hacerla rigurosa desde el punto de vista técnico y tomar las medidas necesarias para que los parámetros del sistema se ajusten. Al respecto se deberá tomar una decisión en relación con los siguientes aspectos: a) Fortaleza de las contraseñas pasando a una cadena de 10 caracteres como mínimo. b) Combinación en una misma contraseña de caracteres alfabéticos, numéricos, letras mayúsculas y minúsculas, así como caracteres especiales, c) Cambio de la contraseña generada por el sistema, una vez que el usuario ingresa por primera vez a la plataforma web, d) Bloqueo del usuario por abandono de equipo (tiempo transcurrido entre consultas o transacciones), e) Reciclaje de contraseñas. Para dar cumplimiento a esta disposición, deberá remitirse a la Contraloría General a más tardar **15 de junio 2021** una certificación en la cual se haga constar que se presentó ante el Consejo Rector los resultados de la valoración efectuada y la propuesta de modificación de la Política de contraseñas, documentos que deberán adjuntarse con la certificación; además, en caso de que procesa, a más tardar el **15 de julio 2021**, una certificación donde consta que dicha política fue debidamente ajustada, divulgada e implementada. (Ver párrafos del 2.34 a 2.44)

4.8. Definir, oficializar e implementar un mecanismo de control complementario relacionado con el principio de segregación de funciones en el equipo de TI del SINIRUBE, el cual incluya los roles, las responsabilidades monitoreo y niveles de aprobación. Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor, a más tardar el **16 de agosto 2021**, una certificación en la cual se haga constar que dicho mecanismo de control fue definido y oficializado, y a más tardar el **30 de noviembre 2021**, una certificación de que dicho mecanismo fue implementado. (Ver párrafos del 2.45 a 2.51)

AL MASTER JUAN LUIS BERMÚDEZ MADRIZ EN SU CALIDAD DE PRESIDENTE DEL CONSEJO RECTOR DEL SINIRUBE O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.9. Someter a valoración y resolución del Consejo Rector del SINIRUBE lo correspondiente en relación con la disposición 4.5. Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor, a más tardar el **28 de febrero 2022**, una certificación en la cual se haga constar que lo correspondiente a esas disposiciones fue valorado, y a más tardar el **29 de abril de 2022**, una certificación de que dichos asuntos fueron resueltos. (Ver párrafos del 2.6 al 2.22)

4.10. Someter a valoración y resolución del Consejo Rector del SINIRUBE lo correspondiente en relación con la disposición 4.7. Para dar cumplimiento a esta disposición, deberá remitirse al Órgano Contralor, a más tardar el **15 de julio 2021**, una certificación en la cual se haga constar que lo correspondiente a esas disposiciones fue valorado, y a más tardar el **13 de agosto de 2021**, una certificación de que dichos asuntos fueron resueltos. (Ver párrafos del 2.34 al 2.44)

Firmado digitalmente por MANUEL JESUS
CORRALES UMAÑA
Fecha: 2021-05-27 22:04

Manuel Corrales Umaña
Gerente de Área

Firmado digitalmente por SILVIA ELENA
LOPEZ VILLALOBOS
Fecha: 2021-05-27 09:36

Silvia López Villalobos
Asistente Técnica

ALEJANDRO ZUÑIGA
GOMEZ (FIRMA)
Firmado digitalmente por
ALEJANDRO ZUÑIGA GOMEZ (FIRMA)
Fecha: 2021.05.27 11:29:10 -06'00'

Alejandro Zúñiga Gómez
Coordinador

Firmado digitalmente por MARIA
JOSE LASCAREZ GRANADOS
Fecha: 2021-05-27 09:28

María José Láscarez Granados
Colaboradora

Firmado digitalmente por JONATHAN
ALONSO ESCALANTE JIMENEZ
Fecha: 2021-05-27 09:49

Jonathan Escalante Jiménez
Colaborador

Anexo nro. 1

Glosario

Término	Concepto
Acuerdo de Servicio	Los acuerdos de servicios, mejor conocidos como convenios o acuerdos de nivel de servicio ("SLA's" por sus siglas en inglés de "Service Level Agreement") son contratos escritos, formales, desarrollados conjuntamente por el proveedor del servicio de TI y los usuarios respectivos, en los que se define, en términos cuantitativos y cualitativos, el servicio que brindará la dependencia responsable de TI y las responsabilidades de la contraparte beneficiada por dichos servicios. (N-2-2007-CO-DFOE)
Amenaza	Cualquier cosa (por ejemplo, un objeto, una sustancia, un ser humano) que sea capaz de actuar contra un activo de una manera que pueda dañarlo. Una causa potencial de un incidente no deseado. (ISO/IEC 13335)
Base de Datos	Colección de datos almacenados en un computador, los cuales pueden ser accedidos de diversas formas para apoyar los sistemas de información de la organización.(N-2-2007-CO-DFOE)
Base de datos de configuraciones	(CMDB por sus siglas en inglés de "Configuration Management database") Base de datos utilizada para almacenar los registros de configuración a lo largo de su ciclo de vida. En la CMDB también se conservan las relaciones entre los registros de configuración. (ITIL V4)
Confidencialidad de la información	Protección de información sensible contra divulgación no autorizada. (N-2-2007-CO-DFOE)
Continuidad de negocio	Prevención, mitigación y recuperación contra las interrupciones. También se pueden usar en este contexto los términos "planes de reanudación de negocios", "planes de recuperación de desastres" y "planes de contingencia"; todos se concentran en los aspectos de recuperación de la continuidad. (ISACA 2015)
Contingencia	Riesgo que afecta la continuidad de los servicios y operaciones. (N-2-2007-CO-DFOE)
Disponibilidad de la información	Se vincula con el hecho de que la información se encuentre disponible (v.gr. utilizable) cuando necesite un proceso de organización en el presente y en el futuro. También se asocia con la protección de los recursos necesarios y las capacidades asociadas. Implica que se cuente con la información necesaria en el momento en que la organización la requiere. (N-2-2007-CO-DFOE)
Hardware	Todos los componentes electrónicos, eléctricos y mecánicos que integran una computadora, en oposición a los programas que se escriben para ella y la controlan (software). (N-2-2007-CO-DFOE)
Integridad	Precisión y suficiencia de la información, así como su validez de

	acuerdo con los valores y expectativas del negocio. (N-2-2007-CO-DFOE)
Migración	Proceso de traslado de datos o sistemas entre plataformas o entre sistemas. (N-2-2007-CO-DFOE)
Parche de seguridad	Aplicativo que permite realizar ajustes a los programas para corregir errores o introducir nuevas funcionalidades de seguridad.
Procesamiento de datos	captura almacenamiento y transformación de grandes cantidades de datos para convertirlo en información valiosa, la acumulación y manipulación de elementos de datos para producir información significativa. (N-2-2007-CO-DFOE)
Riesgo	La combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 73)
Seguridad de información	Garantiza que dentro de la empresa la información esté protegida contra la divulgación a usuarios no autorizados (confidencialidad), la modificación indebida (integridad) y el no acceso cuando se requiere (disponibilidad).
Seguridad Lógica	Se refiere a la seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.
Software	Los programas y documentación que los soporta que permite y que facilitan el uso de la computadora. el software controla la operación del hardware. (N-2-2007-CO-DFOE)
Sistema de alimentación ininterrumpida	(UPS por sus siglas en inglés de “Uninterruptible Power Supply”): Sistema de suministro de energía de respaldo de corto tiempo proveniente de baterías para un sistema de computadora cuando falla la energía eléctrica o la misma cae a un nivel no aceptable de voltaje. (ISACA 2015)
Vulnerabilidad	Deficiencia en el diseño, implementación, operación o el control interno de un proceso que podría exponer al sistema a las adversidades de eventos de amenazas. (ISACA 2014)