INFORME DE AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA SEGURIDAD DE LA INFORMACIÓN EN EL MINISTERIO DE SALUD

29 de mayo de 2023
Informe N.° DFOE-BIS-IAD-00002-2023

División de Fiscalización Operativa y Evaluativa
Área de Fiscalización para el Desarrollo del Bienestar Social
Auditoría de Carácter Especial - Compromiso de informe directo
Contraloría General de la República

CONTENIDO

CUADROS

IMÁGENES

Resumen Ejecutivo

¿QUÉ EXAMINAMOS?

La auditoría tuvo como propósito determinar si la seguridad de la información de los sistemas críticos del Ministerio de Salud responde al marco regulatorio y buenas prácticas aplicables, a efectos de prevenir afectaciones en la prestación de los servicios. El período evaluado comprende desde el 1 de enero de 2021 hasta el 24 de abril de 2023.

¿POR QUÉ ES IMPORTANTE?

El Ministerio de Salud, como ente rector del Sistema Nacional de Salud, encargado de la organización, coordinación y dirección de los servicios de salud, cuenta con sistemas para el apoyo de procesos sustantivos, con los cuales recibe, procesa y genera información. Entre ellos el control de la donación, asignación y trasplante de órganos y tejidos; el registro y evaluación de productos, alimentos y materias primas; y la administración de órdenes sanitarias. Dicha información tiene diversos grados de criticidad y sensibilidad para el cumplimiento de las funciones institucionales.

Así, en aras de garantizar la confidencialidad, integridad y disponibilidad de la información, resulta fundamental el análisis de las medidas con que cuenta dicho Ministerio para proteger la información contra el acceso, uso, divulgación, modificación o destrucción no autorizada; mantener en operación los sistemas e infraestructura tecnológica en la que se encuentran soportados y, en caso de presentarse un incidente, restablecer la información, los sistemas e infraestructura. Aspecto que toma mayor relevancia, al considerar el estado de emergencia declarado en 2022, ante los ataques cibernéticos recibidos por diversas instituciones, entre ellas el propio Ministerio de Salud.

¿QUÉ ENCONTRAMOS?

La Contraloría General determinó que existen debilidades en materia de seguridad de los sistemas y plataformas, así como en la continuidad de las operaciones, las cuales no permiten afirmar que la seguridad de la información de los sistemas críticos del Ministerio de Salud responde al marco regulatorio y buenas prácticas aplicables, a efectos de prevenir afectaciones en la prestación de los servicios.

Al respecto, el Ministerio de Salud ha oficializado normativa en materia de seguridad y ciberseguridad tras el ataque cibernético sufrido en septiembre de 2022; sin embargo, no contempla los incidentes de ciberseguridad dentro de sus procesos de gestión de riesgos institucionales.

Tampoco cuenta con planes de formación para el personal encargado de seguridad de la información, ni planes de sensibilización a los funcionarios acerca del marco de seguridad de la información y gestión de incidentes institucional. Lo señalado, provoca incertidumbre acerca de la ruta a seguir ante una posible vulneración a su ciberseguridad.

Asimismo, se evidenció la existencia de manuales de acceso público en los que se expone información sobre módulos, funcionalidades y estructura de los sistemas, que debe ser conocida únicamente por usuarios internos del propio Ministerio, o de la Caja Costarricense del Seguro Social.

Por su parte, se determinaron debilidades en la gestión integral de los usuarios, relacionadas con la ausencia de controles que garanticen que dichos usuarios están cumpliendo con las medidas de seguridad para el acceso a los equipos y sistemas, establecidas en los lineamientos de ciberseguridad y de contraseñas. También en cuanto a la configuración de las medidas de seguridad para el acceso a los sistemas de información y equipos de cómputo, que impiden verificar la aplicación de los lineamientos de ciberseguridad y de contraseñas

Dichas situaciones facilitan eventuales accesos de individuos no autorizados a los sistemas e infraestructura tecnológica del Ministerio, en perjuicio de la seguridad de la información y la continuidad de los servicios.

También, se determinó que el Ministerio de Salud no ha identificado la información, los sistemas y los dispositivos institucionales críticos para asegurar la continuidad de los servicios, lo cual resulta necesario para establecer controles de seguridad integrales y definir la prioridad de atención que debe dárseles en caso de una interrupción.

Aunado a ello, se encontraron debilidades en la planificación y gestión de los procesos de continuidad de las operaciones y recuperación en caso de incidentes, pues no se han definido aspectos como los niveles de tolerancia ante interrupciones, la ejecución de pruebas a los respaldos y la planificación de contingencias y recuperación ante incidentes. Ello compromete la capacidad de respuesta de ese Ministerio en caso de interrupciones, potenciando los posibles efectos negativos, ante la falta de orientaciones que busquen reducir el tiempo de recuperación y la pérdida de información.

Adicionalmente, se detectaron vulnerabilidades de seguridad en el entorno web del Ministerio de Salud. Las cuales fueron comunicadas a la Administración el 6 de marzo de 2023.

¿QUÉ SIGUE?

Se dispone a las autoridades del Ministerio de Salud, entre otros aspectos, programar e implementar las sesiones del Consejo Tecnológico de ese Ministerio, con el fin de impulsar la toma de decisiones estratégicas en tecnologías de la información y comunicación. Además elaborar e implementar las políticas de seguridad de la información, las políticas de continuidad de negocio; y el cronograma para desarrollar el modelo de arquitectura empresarial del Ministerio de Salud.

Asimismo, se dispone la elaboración e implementación del cronograma para corregir las vulnerabilidades que fueron comunicadas, así como elaborar la propuesta de mecanismo de control para garantizar que el acceso a la información de los manuales de usuario de los sistemas institucionales sea acorde con los roles, funciones y autorizaciones para cada tipo y perfil de usuario.

INFORME DE AUDITORÍA SOBRE LA SEGURIDAD DE LA INFORMACIÓN EN EL MINISTERIO DE SALUD

1. INTRODUCCIÓN

ORIGEN DE LA AUDITORÍA

1.1. El Ministerio de Salud se apoya en herramientas tecnológicas a través de las cuales recibe, procesa y genera información necesaria para el ejercicio de la rectoría del Sistema Nacional de Salud y la prestación de sus servicios. Ello conlleva la activación de mecanismos y controles para proteger la información y mantener disponible la plataforma tecnológica, en procura de la continuidad de las operaciones.

1.2. En 2022, se declaró un estado de emergencia ante los ciberataques recibidos por varias instituciones públicas[1], dentro de las cuales se encuentra el Ministerio de Salud. Por consiguiente, es relevante analizar los controles implementados por ese Ministerio para prevenir, detectar y atender eventos que puedan afectar la seguridad de la información y la continuidad en la prestación de sus servicios.

1.3. La auditoría se realizó en cumplimiento del Plan Anual Operativo de la DFOE y sus modificaciones, con fundamento en las competencias que le son conferidas a la Contraloría General de la República en los artículos 183 y 184 de la Constitución Política y los artículos 12, 17 y 21 de su Ley Orgánica, N.° 7428.

OBJETIVO

1.4. La auditoría tuvo como propósito determinar si la seguridad de la información de los sistemas críticos del Ministerio de Salud responde al marco regulatorio y buenas prácticas aplicables, a efectos de prevenir afectaciones en la prestación de los servicios.

ALCANCE

1.5. La auditoría comprendió el análisis de la gestión de tecnologías de información relacionada con la preparación que tienen el Ministerio de Salud ante posibles

[1] Decreto Ejecutivo N.° 43542-MP-MICIT, Declara estado de emergencia nacional en todo el sector público del Estado costarricense, debido a los cibercrímenes que han afectado la estructura de los sistemas de información, publicado en La Gaceta N.° 86 del 11 de mayo de 2022.

ciberataques, así como de los mecanismos de control que tiene para el resguardo de la información contenida en las bases de datos de los sistemas informáticos. El período de análisis comprendió del 1 de enero de 2022 al 24 de abril de 2023.

CRITERIOS DE AUDITORÍA

1.6. Los criterios de auditoría se presentaron el 23 de enero de 2023 a las funcionarias del Ministerio de Salud María Garino Varela, Asesora del Despacho de la Viceministra; y Petronila Mairena Traña, Jefa de Gestión de Servicios del Departamento de Tecnologías de Información y Comunicación. Posteriormente, fueron comunicados mediante oficio DFOE-BIS-0035 (00958) del 30 de enero de 2023.

METODOLOGÍA APLICADA

1.7. 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, el Procedimiento de Auditoría vigente, establecido por la DFOE, que está basado en la ISSAI 100: Principios Fundamentales de Auditoría del Sector Público, y los principios de la ISSAI 400: Principios de la Auditoría de Cumplimiento de las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI por sus siglas en inglés).

1.8. Para el desarrollo de esta auditoría se utilizó información suministrada en entrevistas y sesiones de trabajo con funcionarios del Ministerio de Salud, así como las respuestas a las consultas planteadas por escrito a ese Ministerio. También, se realizaron pruebas sustantivas para validar la efectividad operativa de controles específicos tanto a nivel de aplicaciones como a nivel de gestión de TI. Además, se realizaron pruebas no intrusivas a la plataforma web en busca de vulnerabilidades conocidas cuyos resultados se reportaron a la administración con carácter confidencial.

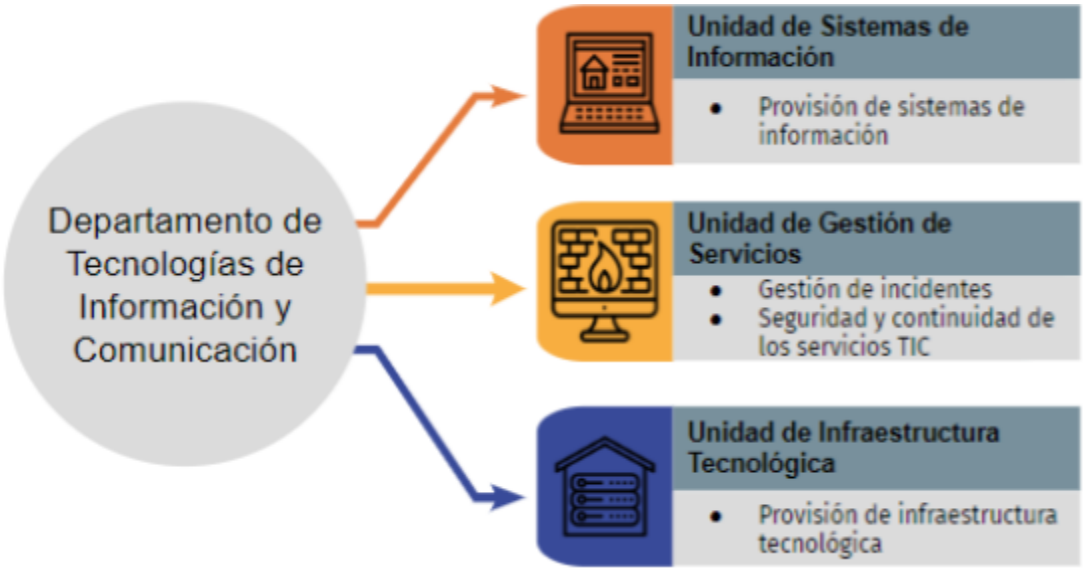
GENERALIDADES ACERCA DEL OBJETO AUDITADO

1.9. El Ministerio de Salud ha definido, como parte de sus políticas institucionales, el uso y fortalecimiento de las tecnologías de información y comunicación para optimizar sus funciones rectoras. Dicho Ministerio tiene una estructura organizacional dividida en tres niveles de gestión: el nivel central, que constituye el nivel político-estratégico y técnico-normativo, y determina la normativa, procedimientos y sistemas para la implementación del marco estratégico institucional; el nivel regional, correspondiente al nivel político-táctico, el cual constituye el enlace entre el nivel central y el nivel local; y el nivel local, que refiere al nivel político-operativo en la ejecución de las funciones sustantivas para el ejercicio de la rectoría y de provisión de servicios de salud.

1.10. En el nivel central, se encuentra la Dirección General de Salud, de la cual depende el Departamento de Tecnologías de Información y Comunicación (DTIC). El objetivo de este departamento es garantizar que las TIC respondan a las necesidades institucionales, mediante el desarrollo y mejoramiento continuo de la seguridad, disponibilidad, integridad

y oportunidad de los sistemas de información, la infraestructura y los servicios, en los tres niveles de gestión, a fin de fortalecer la rectoría y la toma de decisiones.[2] El DTIC está conformado por tres unidades que se muestran en la imagen N.° 1.

Imagen N.° 1. Conformación del Departamento de Tecnologías de Información y Comunicación del Ministerio de Salud



Fuente: elaboración propia con base en el Reglamento Orgánico del Ministerio de Salud N.° 40724-S del 23 de septiembre de 2017 y sus reformas.

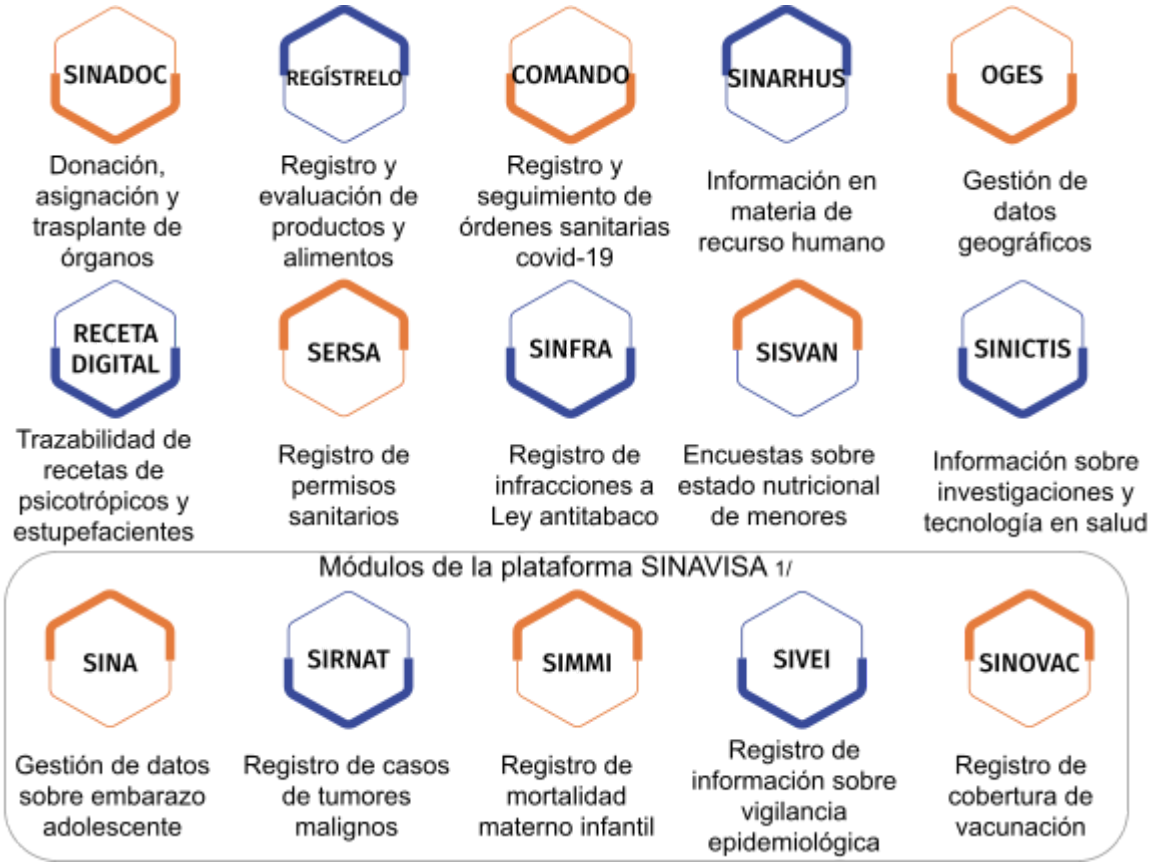
1.11. Como parte de su marco estratégico, el Ministerio de Salud estableció un objetivo relacionado con el fortalecimiento del uso de las tecnologías de información y comunicación para el mejoramiento continuo de la capacidad técnica y operativa de la institución, reducir la brecha tecnológica, la transparencia y la rendición de cuentas[3].

1.12. De esta forma, el Ministerio de Salud se apoya en el uso de al menos 15 sistemas de información e infraestructura tecnológica, para el desarrollo de sus operaciones sustantivas en los tres niveles de gestión[4], tales como el control de la donación, asignación y trasplante de órganos y tejidos; el registro y evaluación de productos, alimentos y materias primas; y la administración de órdenes sanitarias; entre otros que inciden en la salud pública, según se muestra en la imagen N.° 2.

1.13. Adicionalmente, cuenta con otros sistemas de información para el apoyo de procesos internos como la gestión del recurso humano, el control de correspondencia, la planificación institucional y la gestión de auditoría interna, entre otros.

[2] Reglamento Orgánico del Ministerio de Salud N.° 40724-S del 23 de septiembre de 2017 y sus reformas.
[3] Ibidem.
[4] Oficio MS-DTIC-248-2022 del 4 de noviembre de 2022.

Imagen N.° 2. Sistemas que apoyan la labor sustantiva del Ministerio de Salud



1/ SINAVISA es una plataforma por medio de la cual se accede a los cinco sistemas de información indicados en la imagen.
Fuente: Elaboración CGR con base en información suministrada por el Departamento de TIC del Ministerio de Salud.

1.14. En agosto de 2022, el DTIC del Ministerio de Salud creó el Comité Técnico de Seguridad de la Información y Ciberseguridad (CTSIC), compuesto por funcionarios de ese Departamento; cuya finalidad es crear un sistema de gestión de incidentes de seguridad y ciberseguridad institucional para hacerle frente a posibles ataques, amenazas y asegurar la disponibilidad, confidencialidad e integridad de la información, mediante la implementación de una serie de buenas prácticas[5].

1.15. En septiembre de 2022, ese Ministerio sufrió un ciberataque, por el cual se vio obligado a dar de baja algunos servicios y sistemas en forma preventiva, con el fin de detectar posibles intrusiones o accesos no autorizados a equipos, datos e información institucional.

[5] Oficio MS-DTIC-141-2022 del 23 de agosto de 2022.

1.16. De acuerdo con el Ministerio ese ataque no comprometió los servicios ni la información bajo su responsabilidad[6]; sin embargo, a raíz de ello, ha implementado medidas de seguridad a nivel de redes, equipos y plataforma de sistemas, por ejemplo, para restablecer el tráfico de información con la Caja Costarricense del Seguro Social[7]. Asimismo, con base en el Decreto Ejecutivo de emergencia N.° 43542-MP-MICITT, ha gestionado por medio de la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias, la contratación de profesionales especialistas en ciberseguridad[8].

1.17. En lo que concierne al gobierno de las tecnologías de información, en noviembre de 2022 el Ministerio conformó el Consejo Tecnológico[9], como órgano rector institucional en materia de tecnologías de información y comunicación, cuyo propósito es habilitar la gobernanza en torno a las tecnologías de información y comunicaciones. Asimismo, conformó el Equipo de Apoyo[10] al Despacho Ministerial para asuntos relacionados con tecnologías de información y comunicaciones, específicamente en temas relativos a ciberseguridad, infraestructura, interoperabilidad y temas emergentes.

COMUNICACIÓN PRELIMINAR DE LOS RESULTADOS DE LA AUDITORÍA

1.18. En reunión efectuada el 22 de mayo de 2023, en las oficinas centrales del Ministerio de Salud, se presentaron los resultados de la auditoría a la Dra. Mary Munive Angermüller, Ministra de Salud; Edgar Morales González, Director del Departamento de Tecnologías de Información; Sara Pérez Salas, Asesora; José Fabio Aneys Villalobos, Asesor; Cristian Barquero, Asesor; Jonathan Quesada Castillo, Asesor; Carolina Gallo Chaves, Viceministra de Salud; y Miriam Calvo Reyes, funcionaria de la Auditoría Interna.

1.19. El borrador de informe se remitió mediante oficio N.° 06198 (DFOE-BIS-0308) del 16 de mayo de 2023, con el fin de que la Administración hiciera sus observaciones. Al respecto, se recibieron observaciones al borrador de informe en el oficio N.° MS-DM-5916-2023 del 24 de mayo de 2023. Lo resuelto sobre el particular se comunicó mediante oficio N.° (06599) DFOE-BIS-0331 el 26 de mayo de 2023.

[6] Oficio MS-DM-9344-2022 del 13 de octubre de 2022.
[7] Oficio MS-DTIC-248-2022 del 4 de noviembre de 2022.
[8] Oficio CNE-JD-CA-229-2022 del 01 de diciembre de 2022.
[9] Oficio MS-DM-10166-2022 del 17 de noviembre de 2022.
[10] Oficio MS-DM-10168-2022 del 17 de noviembre de 2022.

SIGLAS

1.20. En el cuadro N.°1 se indican las principales siglas utilizadas en este informe y su significado.

Cuadro N.° 1. Siglas utilizadas en el informe

Siglas	Significado
CGR	Contraloría General de la República
DFOE	División de Fiscalización Operativa y Evaluativa de la CGR
DTIC	Departamento de Tecnologías de Información y Comunicación del Ministerio de Salud
SINADOC	Sistema Nacional de Donantes de órganos
SINARHUS	Sistema Nacional de Recursos Humanos en Salud
OGES	Observatorio Geográfico en Salud
SERSA	Sistema Estandarizado de Regulación en Salud
SINFRA	Sistema Nacional de Infractores Tabaco
SISVAN	Sistema de Vigilancia Nutricional en Salud
SINICTIS	Sistema de Ciencia y Tecnología
SINA	Sistema Nacional de Adolescentes
SIRNAT	Sistema Registro Nacional de Tumores
SIMMI	Sistema de Mortalidad Materno e Infantil
SIVEI	Sistema Nacional de Vigilancia Epidemiológica Integrada
SINOVAC	Sistema Nominal de Vacunación
SINAVISA	Sistema Nacional de Vigilancia de la Salud Automatizado

2. RESULTADOS

Seguridad de la información de los sistemas institucionales

Ausencia de gestión de riesgos en ciberseguridad

2.1. La Contraloría General determinó que el Ministerio de Salud no contempla los incidentes de ciberseguridad dentro de su proceso de gestión de riesgos asociados a la seguridad de la información. En ese sentido, tampoco cuenta con planes de capacitación, formación y actualización para el personal encargado de seguridad de la información y ciberseguridad; ni para su promoción en la cultura organizacional.

2.2. Al respecto, la Unidad de Gestión de Servicios del DTIC ha identificado algunas situaciones que podrían generar riesgos en servidores, aplicaciones y documentos; sin embargo estas son exclusivamente del ámbito técnico y no se identifican y analizan formalmente como riesgos. Si bien, tras el hackeo sufrido en septiembre de 2022, la institución ha oficializado normativa en materia de seguridad y ciberseguridad, a la fecha de emisión de este informe, aún no se habían tomado medidas para promover la responsabilidad acerca de la seguridad de la información y ciberseguridad por parte de los funcionarios. Lo anterior, a efectos de que se conozcan e implementen las prácticas de seguridad de la información generales, procedimientos y protocolos de actuación para el reporte y gestión de incidentes conforme a lo plasmado por la institución en su normativa.

2.3. Sobre el particular, el artículo 14 de Ley General de Control Interno N.° 8292 establece el deber de identificar y analizar los riesgos y establecer mecanismos operativos que los minimicen; mientras que el artículo 18 señala el deber de contar con un sistema específico de valoración de riesgo que permita identificar y administrar el nivel de riesgo institucional.

2.4. De igual forma, en las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), específicamente en la norma 3.1, se establece la necesidad de implementar un proceso de valoración de riesgo institucional; y en la norma 5.7.4 se señala la necesidad de instaurar controles para proteger la información, según el grado de sensibilidad y confidencialidad.

2.5. Adicionalmente, las Normas técnicas para la gestión y el control de las tecnologías de información emitidas por el MICITT, actualizadas en 2022, señalan en el apartado I. Gobernanza de TI, el deber de contar con un órgano rector conformado por las autoridades competentes, que tome las decisiones sobre asuntos estratégicos de tecnologías de información; mientras que en el apartado IV. Gestión de riesgos tecnológicos, indican que la institución debe establecer un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales.

2.6. En complemento, en el apartado XI. Seguridad y ciberseguridad, de estas mismas Normas, se establece que la institución debe implementar medidas de control para administrar el riesgo de seguridad de la información y ciberseguridad, que permitan el

cumplimiento de los objetivos de los procesos, protegiendo la confidencialidad, autenticidad, privacidad e integridad de la información; además, debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios, contemplando la participación e involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales. Todo lo anterior, debidamente respaldado en una Política de seguridad de la información y ciberseguridad.

2.7. Cabe señalar que las Políticas de gestión de tecnologías de información y comunicación del Ministerio de Salud, versión 2.1 aprobada en 2019, señalan en el apartado 4.3 la necesidad de prevenir, o bien minimizar, las amenazas a la seguridad, mediante una adecuada gestión de riesgos y normativa.

2.8. Por su parte, las Normas de seguridad de la información del Ministerio de Salud, versión 1.1, de junio de 2017, establecen en la norma 6.8 Responsabilidades con la seguridad de la información, que “El compromiso y responsabilidad en materia de seguridad de la información compete tanto a las Autoridades Superiores como directores, jefes y personal en general” y que “Las Autoridades Superiores, deben hacer de conocimiento a todos los funcionarios de la institución, sobre las responsabilidades que les compete en materia de seguridad y los riesgos que implica la no observancia u omisión de la misma, así como velar por que el personal se capacite en forma permanente e implementar mecanismos de control para el cumplimiento de estas responsabilidades”.

2.9. En adición, las buenas prácticas establecidas en la Norma ISO/IEC 27001:2014 Sistemas de Gestión de Seguridad de Información, indican en el apartado 5.1 Liderazgo y compromiso, que la alta dirección debe demostrar su liderazgo y compromiso con la seguridad de la información, para lo cual debe asegurarse que la política de seguridad de la información y los objetivos de seguridad de la información estén establecidos y sean compatibles con la dirección estratégica de la organización.

2.10. Asimismo, el apartado 5.2 Política, de la citada Norma, señala que la alta dirección debe establecer una política de seguridad de la información que incluya objetivos de seguridad de la información o proporcione el marco para establecerlos; mientras que el apartado 6.1. Acciones para abordar los riesgos y las oportunidades, señala que el proceso de valoración del riesgo institucional debe establecer los criterios de aceptación de riesgo; identificar los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad; así como definir y aplicar un proceso de tratamiento.

2.11. Las situaciones encontradas son atribuibles a la falta de consolidación de un órgano rector en materia de tecnologías y seguridad de la información, lo cual ha impedido definir al menos la tolerancia o límite de riesgo aceptable de la institución, los objetivos de seguridad de la información; la incorporación de eventos de ciberseguridad en los procesos de gestión de riesgos institucionales; la capacitación, formación y actualización para el personal encargado de seguridad de la información y ciberseguridad. También, la sensibilización de las personas funcionarias sobre las normas, prácticas generales,

procedimientos y protocolos institucionales para la seguridad de la información y para el reporte y gestión de incidentes.

2.12. Al respecto, el Ministerio de Salud, en diferentes momentos, ha creado instancias de alto nivel para orientar lo referente a la seguridad de la información[11]. Sin embargo, estas no sesionaron regularmente. La última instancia, conformada en noviembre de 2022, corresponde al Consejo Tecnológico del Ministerio de Salud, como nuevo órgano rector para la gobernanza de tecnologías de información[12].

2.13. En ese sentido, el Ministerio informó a la CGR, en referencia a las anteriores instancias de alto nivel, que la Comisión Gerencial de Tecnologías de Información y Comunicación (CGTIC) no fue convocada a sesionar durante el año 2021; mientras que el posterior Comité Gerencial de Tecnologías de Información y Comunicación del Ministerio de Salud no pudo sesionar debidamente por las múltiples ocupaciones de sus miembros[13].

2.14. En consecuencia, la institución presenta incertidumbre acerca de la ruta a seguir ante una posible vulneración a su ciberseguridad, y carece de medidas de protección y control integrales. Lo cual, a su vez, potencia el riesgo de mayores afectaciones ante un ciberataque; por ejemplo, mayor riesgo de pérdida de información o una prolongación del tiempo que los servicios permanezcan inhabilitados. Asimismo, al carecer de medidas no planificadas, se aumentan los costos de implementar acciones reactivas.

Información del funcionamiento de los sistemas institucionales expuesta

2.15. La Contraloría General determinó que existen manuales de usuario con información crítica de los sistemas del Ministerio de Salud, los cuales se encuentran disponibles al público en sus sitios web, de forma irrestricta, sin obedecer a una segmentación de acceso según roles y perfiles.

2.16. Al respecto, se identificó que nueve de 16 sistemas de información, cuentan con manuales disponibles al público, los cuales incluyen información sobre módulos, funcionalidades y estructura de los sistemas, cuyo uso debe ser únicamente por usuarios internos del propio Ministerio, o de la Caja Costarricense del Seguro Social, según sus roles y funciones.

2.17. Así, a la fecha de emisión de este informe, los manuales se encontraban disponibles para su acceso o descarga desde la página web institucional o desde el sitio web de cada sistema.

2.18. Lo señalado no es congruente con lo establecido en la norma 5.7 de las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), en cuanto al deber de asegurar que la comunicación de la información se dé en las instancias pertinentes, según las necesidades de los usuarios en su esfera de acción. Así como la norma 5.8, la cual

[11] En mayo de 2019 se creó la Comisión Gerencial de Tecnologías de Información (CGTIC); mientras que en enero de 2022, se nombró al Comité Gerencial de Tecnologías de Información y Comunicación del Ministerio de Salud (CGTIC-MS).
[12] Oficio N.° MS-DM-10166-2022 del 17 de noviembre de 2022.
[13] Oficio N.° MS-DTIC-248-2022 del 4 de noviembre de 2022.

señala el deber de administrar los niveles de acceso a la información y datos sensibles, y establecer condiciones de protección apropiadas, según su grado de sensibilidad y confidencialidad.

2.19. Por su parte, las Normas técnicas para la gestión y el control de las tecnologías de información emitidas por el MICITT, actualizadas en 2022, en el apartado XI. Seguridad y Ciberseguridad, señalan deber de establecer mecanismos para que, tanto el personal como terceros, tengan los accesos mínimos necesarios para sus fines, y se asegure la protección de los activos tecnológicos y de información, según una clasificación que establezca los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información.

2.20. Adicionalmente, la norma 6.5 de las Normas de seguridad de la información del Ministerio de Salud[14], indican que se debe asegurar que los funcionarios cuenten con los derechos o claves de acceso a la información acorde al nivel de autorización asociado a sus funciones.

2.21. Asimismo, las buenas prácticas de COBIT, en su versión 2019, establecen en el objetivo de gestión DSS05 que debe existir un aseguramiento de que todos los usuarios tienen derechos de acceso a la información de acuerdo con los requisitos. En ese sentido el objetivo de gestión DSS06, señala que se deben asignar derechos de acceso con base en lo mínimo requerido para realizar las actividades laborales, conforme a los roles de trabajo predefinidos.

2.22. Así, las situaciones expuestas se atribuyen a que el Ministerio de Salud no ha establecido mecanismos que regulen el acceso a los manuales de usuario, de acuerdo con los diferentes roles y perfiles de cada usuario y la sensibilidad de la información para el funcionamiento de los sistemas. Tampoco ha precisado la información que es estrictamente necesaria mantener de acceso público; ni definido una segmentación de los permisos de acceso a la información de dichos documentos, acorde con los roles y perfiles de cada sistema y el medio por el cual cada usuario, según sus permisos, puede acceder a la información del respectivo manual.

2.23. En consecuencia, la información expuesta sobre características del funcionamiento y administración de los sistemas facilita eventuales intrusiones de individuos maliciosos, que pueden afectar la continuidad de sus operaciones; así como la confidencialidad, integridad y disponibilidad de la información contenida en esos sistemas.

Debilidades en la gestión de la seguridad de los sistemas de información

2.24. La Contraloría General determinó la existencia de debilidades en la gestión integral de los usuarios de sistemas de información y equipos de cómputo, que le impiden al DTIC asegurar que los usuarios están cumpliendo con las medidas de seguridad para el acceso a los equipos y sistemas, establecidas en la normativa interna en materia de ciberseguridad y de administración de contraseñas.

[14] Versión 1.1, de junio de 2017.

2.25. Al respecto, 21 sistemas del Ministerio de Salud (considerando tanto sistemas sustantivos como para funciones administrativas) cuentan con un módulo de seguridad, en el cual se pueden realizar las configuraciones para cumplir con la normativa citada; mientras que hay nueve sistemas sin este tipo de módulo, para los cuales se dispone de una aplicación denominada Módulo de Seguridad Integrado (MSI), que administra los perfiles, roles y contraseñas. Sin embargo, a la fecha de emisión de este informe, no hay certeza de si los usuarios cumplen a cabalidad con las disposiciones de seguridad establecidas, en aspectos como la implementación del doble factor de autenticación, la complejidad de las contraseñas y la no utilización de la misma contraseña para varios servicios.

2.26. Asimismo, se determinó la existencia de usuarios genéricos, particularmente para personas con roles de administrador, lo cual impide identificar en las bitácoras a las personas específicas que realizaron determinadas transacciones en los sistemas.

2.27. Adicionalmente, se desarrolló una batería de pruebas manuales con el fin de detectar vulnerabilidades de seguridad en el entorno web de la institución. Dada la sensibilidad de los hallazgos, se remitió un oficio de acceso restringido a ese Ministerio con el detalle de los resultados obtenidos, a efectos de que realizara una valoración oportuna de las situaciones identificadas y definiera la procedencia de implementar medidas y controles de seguridad[15]. A partir de ello, la Administración determinó algunos ajustes que pueden ser realizados por parte del DTIC, y otros que requieren ser atendidos por los proveedores de los distintos sistemas.

2.28. De esta forma, las situaciones expuestas no son congruentes con el artículo 12 de la Ley General de Control Interno, N.° 8292, en lo referente al deber de tomar acciones correctivas ante cualquier evidencia de desviaciones. Tampoco con lo establecido en la norma 5.7.4 y 5.8 de las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), en cuanto al deber de instaurar controles para proteger la información, según su grado de sensibilidad y confidencialidad, así como disponer de controles para que los sistemas de información garanticen razonablemente su calidad, la seguridad, administración de niveles de acceso y garantía de confidencialidad de la información que ostente ese carácter.

2.29. Asimismo, la política 4.3 de las Políticas de gestión de tecnologías de información y comunicación del Ministerio de Salud[16], indica que deben prevenirse, o bien minimizarse, las amenazas a la seguridad. Mientras que la norma 6.8.2 de las Normas de seguridad de la información de ese Ministerio de Salud[17], señalan el deber de velar por la efectividad de los controles de seguridad de la información.

2.30. Por su parte, los Lineamientos institucionales sobre ciberseguridad LTIC-CS-001, versión 001, de octubre del 2022, establecen en su apartado 5.1 la responsabilidad de mantener actualizados los equipos y la obligatoriedad de cumplir todo dispuesto en los lineamientos. En ese sentido, el apartado 7 incisos g) h), i), j), del Lineamiento para el uso y

[15] Oficio N.° 02550 (DFOE-BIS-0149) del 6 de marzo de 2023.
[16] Versión 2.1, aprobada en 2019.
[17] Versión 1.1, aprobada en 2017.

administración de contraseñas del Ministerio de Salud, versión 1.1 de marzo de 2023, establecen que en cada servicio deben ser utilizadas contraseñas distintas, las reglas a cumplir por las personas funcionarias de los tres niveles para establecer y actualizar las contraseñas, así como las características de longitud y complejidad de las contraseñas.

2.31. En línea con ello, el apartado 10 inciso b) del citado Lineamiento, también establece la responsabilidad del DTIC de velar por que los equipos de cómputo se encuentren debidamente configurados, actualizados y cuenten con las medidas de seguridad establecidas.

2.32. Sobre el particular, el marco de prácticas de COBIT, en su versión 2019, señalan, en el objetivo de gestión DSS06, el deber de definir y mantener controles para garantizar la integridad y seguridad de la información tratada en los procesos de la organización.

2.33. Ahora bien, las situaciones identificadas obedecen a que el Ministerio de Salud no cuenta con instrumentos para verificar la aplicación integral de los lineamientos de ciberseguridad y contraseñas en los equipos de cómputo y los sistemas institucionales, el uso del doble factor de autenticación, así como la identificación en forma precisa de los usuarios y sus transacciones, en las bitácoras de los sistemas. Además, no ha definido de manera precisa las condiciones, acciones ni responsables, para garantizar condiciones mínimas de seguridad de los sistemas de información, que aseguren su resguardo y la continuidad en la prestación de los servicios.

2.34. De esta forma, las debilidades en la gestión de usuarios de sistemas y equipos de cómputo, así como las vulnerabilidades comunicadas pueden provocar accesos indebidos a información sobre la infraestructura y configuración de los sistemas, las cuales pueden ser explotadas por atacantes para afectar su funcionamiento y la continuidad de los servicios, así como la confidencialidad y disponibilidad de la información. Asimismo, la existencia de usuarios genéricos no permite asegurar que el acceso o ajustes en los sistemas sean ejecutados por los usuarios con los roles y autorizaciones para ello, ni identificar a la persona específica que los ejecutó.

Continuidad de las operaciones y recuperación ante incidentes

No se ha identificado la información, sistemas y dispositivos institucionales críticos para la continuidad de los servicios

2.35. Se determinó que el Ministerio de Salud carece de una clasificación y alineación, formal y completa, de los procesos de la institución, la información, sistemas y dispositivos informáticos institucionales, que son críticos para asegurar la continuidad de los servicios. Dicha clasificación resulta necesaria para determinar a cuáles se les debe dar prioridad de restablecimiento en caso de interrupción.

2.36. Si bien, la institución cuenta con un inventario de sistemas, no identifica la información crítica o sensible que se captura, procesa o almacena a través de ellos. Asimismo, en lo concerniente a los dispositivos informáticos, ese Ministerio cuenta con inventarios de

computadoras personales, equipos de telecomunicaciones y servidores; sin embargo, no contiene la totalidad de dispositivos informáticos de la institución, ni contempla una categorización por criticidad.

2.37. Al respecto, la norma 5.9 de las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE) señala el deber de observar la normativa relacionada con tecnologías de información e instaurar mecanismos y procedimientos para garantizar la operación continua y correcta de los sistemas de información.

2.38. Por su parte, las Normas Técnicas para la gestión y el control de las tecnologías de información[18], señalan en el apartado V, que "la entidad debe contar con un modelo de arquitectura que permita visualizar adecuadamente la estructura de procesos institucionales y la relación de uso de recursos instalados (sistemas de información, infraestructura tecnológica) para gestionar los datos e información requeridos en la operativa", así como "disponer de un modelo de clasificación de datos e información, según criterios y requisitos legales, de valor, según el nivel de criticidad y susceptibilidad a divulgación o modificación no autorizada".

2.39. Ese mismo apartado, las Normas citadas refieren a la responsabilidad del órgano rector de gobernanza en TI, de establecer el modelo de arquitectura empresarial, y que la unidad de tecnologías de información debe basarse en el modelo de clasificación de datos e información para establecer las directrices de seguridad y protección de datos e información.

2.40. Complementariamente, esas Normas en su apartado XII, señalan el deber de mantener los activos de tecnologías de información identificados y clasificados según el nivel de criticidad, características y medidas de protección asociadas. Mientras que el apartado XIII, indica que la identificación y análisis de procesos y activos críticos constituyen la base para disponer de un plan de continuidad.

2.41. El propio Ministerio de Salud, en la política 4.2 de sus Políticas de gestión de tecnologías de información y comunicación[19], establece que se debe implementar y mantener tecnologías de información y comunicación manteniendo un estándar de arquitectura e infraestructura tecnológica.

2.42. En línea con ello, las buenas prácticas de COBIT, en su versión 2019, en el objetivo de gestión APO03, refieren al deber de establecer una arquitectura común que consiste en capas de arquitectura de procesos de negocio, información, datos, aplicaciones y tecnología y sus interrelaciones, para posibilitar una prestación estándar, responsable y eficiente de los objetivos operativos y estratégicos.

2.43. Las debilidades señaladas obedecen a que el Ministerio carece de un modelo de arquitectura empresarial (MAE), elaborado con base en un análisis de impacto en el negocio (BIA), el cual le permita identificar la alineación del software, hardware e información, y sus requisitos operativos, con los procesos institucionales, así como el

[18] Emitidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, actualizadas en 2022.

[19] Versión 2.1 aprobada en 2019.

impacto que tendría la institución -y el público receptor de sus servicios- en caso de no estar disponibles durante un período prolongado. Es decir, se carece de un modelo que permita entender los procesos, sus partes constitutivas, la información y tecnología que los respalda, y clasificarlos según su criticidad o impacto en el negocio.

2.44. La ausencia de dicho modelo dificulta el establecimiento de controles integrales y estandarizados -con base en su criticidad- en la información, los sistemas y los dispositivos informáticos necesarios para la ejecución de los procesos institucionales. Ello, a su vez, aumenta el riesgo de que, ante un ciberataque o cualquier otro evento que atente contra la continuidad de las operaciones, efectivamente ocurra una interrupción en los servicios y se potencien las consecuencias que ello puede tener, en cuanto a la pérdida de confidencialidad, integridad y disponibilidad de la información y la disminución en la calidad del servicio a las partes interesadas.

Debilidades en la planificación y gestión de la continuidad de las operaciones y la recuperación ante incidentes

2.45. Se determinó que el Ministerio de Salud no ha definido los elementos necesarios para garantizar razonablemente la continuidad de las operaciones y la recuperación ante incidentes, en lo que respecta a la definición de los niveles de tolerancia de la institución ante interrupciones, la realización de pruebas de los respaldos y la elaboración de planes de contingencias de tecnologías de información y recuperación ante incidentes. Dichos elementos resultan necesarios para responder a incidentes no planificados como desastres naturales, cortes de electricidad, ataques cibernéticos y cualquier otro evento disruptivo.

2.46. Al respecto, el Ministerio carece de una definición de métricas que permitan determinar los niveles de tolerancia de la institución ante interrupciones y sus objetivos de continuidad. Por ejemplo, el objetivo de tiempo de recuperación o RTO (tiempo esperado para recuperar uno o varios sistemas, luego de una interrupción), el objetivo de punto de recuperación o RPO (punto al que se espera recuperar los datos, tomando como base la pérdida de datos aceptable en caso de interrupción), o la ventana de interrupción (período máximo que puede esperar la organización desde el momento de la interrupción hasta la restauración de los servicios o sistemas críticos).

2.47. Además, se determinó que la institución no realiza pruebas para verificar que los respaldos externos de información que ejecuta de sus sistemas son funcionales, y permiten restaurar los posibles servicios críticos.

2.48. Sobre el particular, el apartado XIII de las Normas técnicas para la gestión y el control de las tecnologías de información emitidas por el MICITT, señalan que la institución debe establecer prácticas formales para valorar la resiliencia institucional, disponer de una estrategia viable para mantener la continuidad de las operaciones y la recuperación ante un desastre o incidente, que establezca los roles y responsabilidades adecuadas para responder a situaciones adversas.

2.49. Por su parte, es pertinente señalar que el objetivo de gestión DSS04 de las buenas prácticas de COBIT versión 2019, refieren al deber de definir la política de continuidad del negocio; establecer el tiempo mínimo necesario para recuperar un proceso de negocio y el entorno de tecnologías de información que lo soporta, conforme a una duración aceptable de interrupción y la suspensión tolerable máxima; y documentar todos los procedimientos necesarios para que la organización continúe con sus actividades críticas en caso de incidente.

2.50. En línea con ello, las buenas prácticas establecidas en la norma INTE ISO 22301:2015 Sistemas de gestión de continuidad del negocio, señalan en el apartado 3.4, que la gestión de la continuidad del negocio debe proporcionar un marco para la construcción de la resiliencia organizacional y la capacidad de dar una respuesta efectiva que salvaguarde los intereses de las partes interesadas y las actividades que crean valor.

2.51. Ahora bien, cabe indicar que las debilidades señaladas se atribuyen a que el Ministerio de Salud carece de políticas de continuidad del negocio como marco de referencia para establecer los objetivos de continuidad del negocio y dar trazabilidad a los lineamientos, protocolos y planes, tanto de los procesos de la función sustantiva del Ministerio como del proceso de tecnologías de información, con las intenciones y orientaciones de la organización emanadas por la alta dirección.

2.52. Lo anterior, con el fin de definir los umbrales de riesgo aceptables y las métricas para determinar los niveles de tolerancia a interrupciones de la institución; las orientaciones para disponer de una estrategia viable y rentable para mantener la continuidad de las operaciones, la recuperación ante un desastre y la respuesta a incidentes.

2.53. Además, carece de un procedimiento que permita definir los respaldos que deben ser probados, las actividades para validar la integridad de los datos contenidos en el respaldo, la frecuencia de ejecución de las pruebas, los responsables de ejecutarlas y las actividades para reportar los resultados.

2.54. Como consecuencia, de presentarse un evento adverso que provoque una interrupción, la capacidad de respuesta de ese Ministerio puede verse comprometida, potenciando los posibles efectos negativos, al tiempo de aumentar el riesgo de que el incidente puede provocar una mayor afectación, ante la falta de orientaciones que busquen reducir el tiempo de recuperación y la pérdida de información.

3. CONCLUSIÓN

3.1. El Ministerio de Salud, como ente rector en materia de salud pública, custodia y administra información sensible sobre la salud de las personas, así como de sus funciones relativas a la definición de políticas nacionales de salud. Para ello, ha apoyado sus procesos en sistemas de información.

3.2. Posterior al ciberataque recibido en septiembre de 2022, el Ministerio ha adoptado una serie de medidas, con el fin de prevenir y gestionar futuros incidentes de ciberseguridad. Sin embargo, a partir de la situación encontrada, no es posible afirmar que, a la fecha de emisión de este informe, la seguridad de la información de los sistemas críticos del Ministerio de Salud responda al marco regulatorio y buenas prácticas aplicables, a efectos de prevenir afectaciones en la prestación de los servicios.

3.3. A nivel de seguridad de la información, es importante que la Administración impulse acciones desde el Consejo Tecnológico del Ministerio de Salud, como actual órgano rector para la gobernanza de tecnologías de información, que promuevan la incorporación de prácticas de seguridad de la información y ciberseguridad como un componente transversal de los procesos y la cultura institucionales, y el conocimiento de la normativa atinente que el Ministerio ha emitido. Así, de esa manera, promover la comprensión de que la seguridad de la información, incluyendo lo relativo a ciberseguridad, es una responsabilidad compartida por todas las personas funcionarias, y no una función exclusiva del Departamento de Tecnologías de Información.

3.4. Además, en lo concerniente a la continuidad de las operaciones y la recuperación ante incidentes, es oportuno que el Consejo Tecnológico, al contar con representación de distintos actores del Ministerio, identifique cuáles son los procesos críticos institucionales y sus objetivos de continuidad, para que las acciones definidas por el Departamento de Tecnologías de Información y Comunicación, para procurar la continuidad de los sistemas de información y la infraestructura en que operan, respondan efectivamente a las intenciones y orientaciones de la alta dirección.

3.5. Por último, es pertinente señalar que las acciones dirigidas a fortalecer los elementos desarrollados en el presente informe pueden impulsar el robustecimiento de las estrategias de seguridad de la información y continuidad de las operaciones en el Ministerio de Salud. Lo anterior, de forma tal que se cuente con una mejor preparación ante intentos de ciberataque o cualquier otro evento que atente contra la seguridad y continuidad de sus servicios.

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.

A LA DOCTORA MARY MUNIVE ANGERMÜLLER, EN SU CALIDAD DE MINISTRA DE SALUD, O QUIEN EN SU LUGAR OCUPE EL CARGO

4.4. Elaborar e implementar un cronograma para corregir las vulnerabilidades que le fueron comunicadas mediante oficio N.° 02550 (DFOE-BIS-0149) del 6 de marzo de 2023. Remitir a la CGR una certificación en la cual se acredite la elaboración del cronograma a más tardar el 9 de junio de 2023; así como una certificación acerca de la implementación del cronograma para corregir las vulnerabilidades a más tardar el 23 de junio de 2023. (Ver párrafo 2.24 al 2.34).

A LA DOCTORA MARY MUNIVE ANGERMÜLLER, EN SU CALIDAD DE MINISTRA DE SALUD Y PRESIDENTA DEL CONSEJO TECNOLÓGICO DEL MINISTERIO DE SALUD, O QUIEN EN SU LUGAR OCUPE EL CARGO

4.5. Elaborar, oficializar e implementar la programación de las sesiones del Consejo Tecnológico del Ministerio de Salud, para que este ejecute de manera continua las funciones que le fueron definidas en materia de toma decisiones sobre temas estratégicos asociados con las tecnologías de información y comunicación que inciden en la prestación de los servicios a los usuarios. Remitir a la Contraloría General una certificación, a más tardar el 30 de junio de 2023, que acredite la elaboración y oficialización de la programación de reuniones de dicho Consejo. Asimismo, remitir una certificación, a más tardar el 21 de julio de 2023, donde se acredite la implementación de esa programación. (Ver párrafo 2.1 al 2.14).

AL LICENCIADO EDGAR MORALES MORALES GONZÁLEZ, EN CALIDAD DE DIRECTOR DEL DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DEL MINISTERIO DE SALUD, O QUIEN EN SU LUGAR OCUPE EL CARGO

4.6. Elaborar una propuesta de mecanismo de control para garantizar que el acceso a la información de los manuales de usuario de los sistemas institucionales corresponda a aquella estrictamente necesaria según el rol, funciones y autorización de cada tipo y perfil de usuario. Enviar dicha propuesta al Consejo Tecnológico del Ministerio de Salud para lo de su competencia. Remitir a la Contraloría General una certificación en la cual conste la elaboración y remisión de la propuesta de mecanismo de control al Consejo Tecnológico, a más tardar el 7 de julio de 2023. (Ver párrafo 2.15 al 2.23).

4.7. Elaborar e implementar un mecanismo de control para verificar la aplicación integral de los lineamientos de ciberseguridad y contraseñas en la totalidad de los equipos de cómputo y los sistemas del Ministerio de Salud, el doble factor de autenticación, así como la identificación en forma precisa de los usuarios y sus transacciones, en las bitácoras de los sistemas. Remitir a la Contraloría General de la República una certificación en la cual se acredite la elaboración del mecanismo de control a más tardar el 8 de septiembre de 2023; así como una certificación acerca de la implementación de dicho mecanismo a más tardar el 8 de diciembre de 2023. (Ver párrafo 2.24 al 2.34).

4.8. Elaborar, oficializar e implementar un procedimiento para ejecución de pruebas a los respaldos externos de la información de los sistemas críticos del Ministerio de Salud, que considere al menos, actividades, responsables, y periodicidad de las pruebas. Remitir a la Contraloría General de la República una certificación en la cual conste la elaboración y oficialización del procedimiento para ejecutar las pruebas a los respaldos, a más tardar el 6 de octubre de 2023. Además una certificación acerca de la implementación de las pruebas, al 15 de diciembre de 2023. (Ver párrafo 2.45 al 2.54).

4.9. Elaborar, oficializar, divulgar e implementar un plan de atención de contingencias tecnológicas y recuperación ante incidentes, que contenga, al menos, la definición de roles y responsabilidades, procedimientos de contingencia y recuperación de sistemas e información, métricas u objetivos de recuperación para la información y sistemas, así como pruebas para verificar el funcionamiento y actualización del plan. Remitir a la Contraloría General de la República una certificación en la cual conste la elaboración, oficialización y divulgación del plan para la atención de contingencias tecnológicas y recuperación ante incidentes, a más tardar el 8 de diciembre de 2023. Además, un informe de avance acerca de las medidas iniciadas para implementar el plan al 8 de marzo de 2024. (Ver párrafo 2.45 al 2.54)

AL CONSEJO TECNOLÓGICO DEL MINISTERIO DE SALUD

4.10. Elaborar, formalizar, divulgar e implementar políticas de seguridad de la información para el Ministerio de Salud, que contemplen al menos, una definición institucional de la tolerancia o límite de riesgo y objetivos de seguridad de la información; incorporación de eventos de ciberseguridad en los procesos de gestión de riesgos institucionales; la capacitación, formación y actualización para el personal encargado de seguridad de la información y ciberseguridad; así como la sensibilización a los funcionarios acerca del marco de seguridad de la información institucional. Remitir a la Contraloría General de la República una certificación en la cual conste la elaboración, formalización y divulgación de las políticas, a más tardar el 22 de noviembre de 2023. Además una certificación acerca del inicio de la implementación de las políticas, al 22 de febrero de 2024. (Ver párrafos 2.1 al 2.14).

4.11. Resolver acerca de la aprobación, implementación y divulgación de la propuesta de mecanismo de control para garantizar que el acceso a la información de los manuales de usuario de los sistemas institucionales, corresponda a aquella estrictamente necesaria

según el rol, funciones y autorización de cada tipo y perfil de usuario, que le remita el Director del Departamento de Tecnologías de Información y Comunicación del Ministerio de Salud. Remitir a la Contraloría General una certificación en la cual conste lo resuelto con respecto a la aprobación e implementación de la propuesta de mecanismo de control, a más tardar el 7 de septiembre de 2023. Además, remitir una certificación acerca de la divulgación de la implementación de dicho mecanismo a más tardar el 2 de octubre de 2023. (Ver párrafos 2.15 al 2.23).

4.12. Elaborar, aprobar e implementar un cronograma para desarrollar el modelo de arquitectura empresarial del Ministerio de Salud, que incluya al menos, actividades, responsables, fechas de inicio y finalización, así como los recursos requeridos. Remitir a la Contraloría General de la República, una certificación acerca de la elaboración y aprobación del cronograma para el desarrollo del modelo de arquitectura empresarial, a más tardar el 23 de octubre de 2023. Además, dos informes de avance de la implementación del cronograma, el primero a más tardar el 22 de febrero de 2024, y el segundo al 21 de junio de 2024. (Ver párrafos 2.35 al 2.44).

4.13. Elaborar, oficializar, divulgar e implementar la política de continuidad de negocio que cubra todos los procesos de negocio del Ministerio de Salud y los sistemas de información que los soportan. Remitir a la Contraloría General de la República un informe de avance acerca de la elaboración de la política de continuidad de negocio, a más tardar el 6 de noviembre de 2023, y una certificación en la cual conste la oficialización y divulgación de la política de continuidad de negocio, al 7 de febrero de 2024. Además una certificación acerca del inicio de la implementación de la política, al 22 de abril de 2024. (Ver párrafos 2.45 al 2.54).

Firmado digitalmente por MANUEL JESUS CORRALES UMAÑA
Fecha: 2023-05-29 10:43

Manuel Corrales Umaña
Gerente de Área

Firmado digitalmente por MARVIN MEJIA VARGAS
Fecha: 2023-05-29 09:51

Marvin Mejía Vargas
Asistente Técnico

Firmado digitalmente por ALEX FABIAN RAMIREZ ALPIZAR
Fecha: 2023-05-29 09:42

Alex Fabián Ramírez Alpízar
Coordinador

Firmado digitalmente por MICHEL NAYELY CANUL BOLAÑOS
Fecha: 2023-05-29 09:42

Michel Nayely Canul Bolaños
Colaboradora