INFORME N.° DFOE-PG-IF-21-2017
21 de diciembre, 2017

DIVISIÓN DE FISCALIZACIÓN OPERATIVA Y EVALUATIVA

ÁREA DE FISCALIZACIÓN DE SERVICIOS PÚBLICOS GENERALES

INFORME DE LA AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA CALIDAD Y SEGURIDAD DE LA INFORMACIÓN PARA LA TOMA DE DECISIONES GERENCIALES DE LOS PROCESOS SUSTANTIVOS DE LA DIRECCIÓN GENERAL DE MIGRACIÓN Y EXTRANJERÍA.

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

CONTENIDO

Página nro.

INFORME N.° DFOE-PG-IF-21-2017

RESUMEN EJECUTIVO

¿Qué examinamos?

La auditoría de carácter especial tuvo como objetivo verificar el cumplimiento de buenas prácticas en materia de gestión y control de la calidad y seguridad de la información utilizada para la toma de decisiones gerenciales de los procesos sustantivos de la Dirección General de Migración y Extranjería, de conformidad con el marco normativo y técnico aplicable, nacional e internacional.

¿Por qué es importante?

La Dirección General de Migración y Extranjería es un pilar fundamental para la garantía de la seguridad ciudadana y la lucha contra el crimen organizado. Para realizar su labor de forma eficaz, requiere de información de calidad que le permita tomar decisiones ágiles, tanto estratégicas como operativas. Además, los procesos institucionales y la información en que estos se basan son aspectos sumamente sensibles para la seguridad nacional, y el control efectivo de las entradas y salidas del país en un ambiente altamente riesgoso y susceptible a intereses ligados a actividades ilícitas.

¿Qué encontramos?

La Dirección General de Migración y Extranjería presenta debilidades importantes en la calidad de la información, que dificultan la toma de decisiones tanto estratégicas como operativas, lo cual se debe a la falta de alineamiento de los objetivos de la Gestión de Tecnologías de Información con la estratégica institucional. Además, la Dirección General de Migración y Extranjería no cuenta con un modelo de información que permita integrar de forma eficaz sus sistemas y mantener el nivel de calidad de la información requerido para la toma de decisiones, calidad que también se ve afectada al no ser gestionada de manera explícita. Asimismo, las unidades funcionales de la citada Dirección dependen de forma directa de la intervención de la Gestión de Tecnologías de Información para la confección de información agregada para la toma de decisiones.

También se hallaron debilidades en cuanto a la seguridad de la información. Se presenta una vulnerabilidad dado que Gestión de Tecnologías de Información no cuenta con información inmediata para variar los derechos de acceso a la información de funcionarios que cambian su situación laboral dentro de la Dirección General de Migración y Extranjería, lo cual puede llegar a permitir la manipulación de información confidencial, sensible y relevante por parte de personas que ya no deberían tener estos privilegios.

Otro aspecto de vulnerabilidad a la seguridad de la información encontrado, se relaciona con la continuidad de los servicios que brinda la Dirección General de Migración y Extranjería, los cuales se ven en peligro al no existir planes completos que garanticen que las actividades críticas no van a sufrir detrimento cuando se presente una interrupción de la plataforma tecnológica. Dentro de estas funciones existen actividades tan críticas como la salida de menores del país, impedimentos de salida o entrada, verificación de documentos de viaje, entre otras.

Por último, también se verificó una debilidad de seguridad de la información que representa un riesgo para la plataforma tecnológica, al existir versiones diferentes de software de base (sistemas operativos) en productos similares, lo que dificulta las actualizaciones y estandarización de esta plataforma, así como la existencia de aplicaciones obsoletas, algunas de ellas inclusive sin respaldo del fabricante.

¿Qué sigue?

Se le dispone a la Junta Administrativa de la Dirección General de Migración y Extranjería, elaborar, aprobar y divulgar un Plan Estratégico de Tecnologías de información el cual esté alineado con la estrategia institucional; así como el establecimiento de lineamientos para que cuando se emitan modificaciones al Plan Estratégico Institucional, el Plan Estratégico de Tecnologías de Información se mantenga alineado con la estrategia institucional. También se solicita revisar, ajustar y oficializar el plan de continuidad de negocio y alinearlo con el plan de recuperación de desastres, tomando en cuenta el análisis de impacto de negocio basado en un análisis completo de los riesgos relevantes de la institución; además, confeccionar y aprobar un modelo de arquitectura de información que apoye la integración y calidad de la información que se mantiene en los sistemas de información institucionales y los procedimientos para mantenerlo actualizado.

Se giran disposiciones a la Directora General de Migración y Extranjería, para que se defina, apruebe e implemente un procedimiento de carácter obligatorio mediante el cual las unidades usuarias, incluido el Departamento de Recursos Humanos, informen a Gestión de Tecnologías de Información en el momento en que se produzca cualquier movimiento de personal que involucre la confección, modificación o eliminación de privilegios para acceder a la información institucional; así como la obligatoriedad de que Gestión de Tecnologías de Información realice las modificaciones respectivas de forma inmediata. También, establecer mecanismos de control para velar por el estricto cumplimiento del procedimiento de actualización de permisos de acceso a la información institucional, con el propósito de que, en los casos que se presenten desviaciones, se tomen las acciones correctivas que correspondan.

Por último, se giran una serie de disposiciones a la Gestora de Tecnologías de información, con el fin de que se elabore e implemente: un sistema de gestión de calidad de la información que garantice razonablemente la verificación de los atributos de la información y su mejora continua para la toma de decisiones institucionales; herramientas para que los usuarios finales puedan extraer, de las bases de datos institucionales, la información relevante acorde con sus funciones, con el propósito de que puedan generar sus propios informes para la toma de decisiones de manera oportuna; un procedimiento para la utilización de un ambiente de pruebas permanente para las actualizaciones de software, así como realizar las actualizaciones y migraciones de los sistemas operativos que procedan, para minimizar la exposición a vulnerabilidades procedentes de software desactualizado, obsoleto o sin respaldo del fabricante; así como, definir e implementar procedimientos para mantener actualizados, en forma permanente, todos los documentos y software que respaldan la gestión de tecnologías de información a todo nivel.

INFORME Nro. DFOE-PG-IF-21-2017

DIVISIÓN DE FISCALIZACIÓN OPERATIVA Y EVALUATIVA

ÁREA DE FISCALIZACIÓN DE SERVICIOS PÚBLICOS GENERALES

INFORME DE LA AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA CALIDAD Y SEGURIDAD DE LA INFORMACIÓN PARA LA TOMA DE DECISIONES GERENCIALES DE LOS PROCESOS SUSTANTIVOS DE LA DIRECCIÓN GENERAL DE MIGRACIÓN Y EXTRANJERÍA

1. INTRODUCCIÓN

ORIGEN DE LA AUDITORÍA

1.1. La auditoría se realizó con fundamento en las competencias que le confieren a la Contraloría General los artículos 183 y 184 de la Constitución Política de la República de Costa Rica, así como los artículos 17, 21 y 37 de su Ley Orgánica Nro. 7428.

OBJETIVO DE LA AUDITORÍA

1.2. Verificar el cumplimiento de buenas prácticas en materia de gestión y control de la calidad y seguridad de la información utilizada para la toma de decisiones gerenciales de los procesos sustantivos de la Dirección General de Migración y Extranjería (DGME), de conformidad con el marco normativo y técnico aplicable, nacional e internacional.

ALCANCE DE LA AUDITORÍA

1.3. La auditoría comprendió las medidas de gestión y control diseñadas e implementadas por la administración, para asegurar la calidad y seguridad de la información que soporta la toma de decisiones gerenciales relacionadas con los procesos sustantivos institucionales. El período abarcó las operaciones del 1 de enero de 2016 al 30 de junio de 2017.

GENERALIDADES ACERCA DE LA AUDITORÍA

1.4. La DGME es una institución adscrita al Ministerio de Gobernación y Policía, creada mediante la Ley N.° 7033 del 4 de agosto de 1986, la cual fue derogada posteriormente en su totalidad por la Ley N.° 8487 del 22 de noviembre de 2005, y actualmente se rige por la Ley General de Migración y Extranjería, Ley N.° 8764, publicada en La Gaceta N.° 170 del 1° de setiembre de 2009.

1.5. De acuerdo con su misión, la DGME es el ente público ejecutor de la Política Migratoria, que controla el ingreso y egreso de personas al territorio nacional, promueve la integración de las personas extranjeras a la sociedad costarricense, regula la permanencia y actividades de las personas extranjeras en el país y coadyuva en el combate contra los delitos de trata de personas y tráfico ilícito de migrantes, mediante la administración efectiva de los flujos migratorios que contribuyan al desarrollo y la seguridad de Costa Rica.

1.6. En este escenario, las decisiones que se toman en la DGME deben estar basadas en información oportuna y de calidad, para garantizarle razonablemente a la población, una correcta ejecución de la Política Migratoria y un impacto positivo en la seguridad ciudadana.

METODOLOGÍA APLICADA

1.7. Se utilizó el procedimiento de auditoría vigente de la División de Fiscalización Operativa y Evaluativa y el Manual General de Fiscalización Integral, de la Contraloría General de la República.

COMUNICACIÓN PRELIMINAR DE RESULTADOS DE LA AUDITORÍA

1.8. La comunicación preliminar de los principales resultados, conclusiones, disposiciones y recomendación, producto de la auditoría a que alude el presente informe, se efectuó el 6 de diciembre de 2017, en la sala de reuniones de la Dirección General de Migración y Extranjería; actividad a la que se convocó mediante los oficios N.º 15185 (DFOE-PG-0619) y 15186 (DFOE-PG-0620), ambos del 5 de diciembre de 2017.

1.9. Se contó con la presencia de los siguientes funcionarios: Licda. Lilliam Jarquín Morales, Presidenta de la Junta Administrativa de la DGME; Lic. Esteban Obando Ramos, Sub Director General de Migración y Extranjería; Licda. Jenny Gamboa Rodríguez, Gestora de Tecnologías de Información; todos funcionarios de la DGME, así como los funcionarios de la Auditoría Interna del Ministerio de Gobernación y Policía, Licda. Enid Araya Ramírez y Lic. Jorge González.

1.10. En dicha reunión y en cumplimiento de las "Directrices para la remisión del borrador del informe de fiscalización posterior", por medio de los oficios oficios N.º DFOE-PG-0624 (15213), DFOE-PG-0622 (15210) y DFOE-PG-0623 (15212), se entregó copia digital del borrador del presente informe, a la señora Presidenta de la Junta Administrativa, al señor Sub Director General (dirigida a la señora Directora General, Gisela Yockchen Mora) y a la señora Gestora de Tecnologías de Información, a efecto de obtener las observaciones y sustento documental que la Administración tuviera al respecto.

1.11. Mediante el oficio N.° DG-2534-12-2017 del 13 de diciembre de 2017, el Sub Director General de la DGME indicó que su Despacho no tenía observaciones sobre el contenido del borrador de informe.

2. RESULTADOS

INFORMACIÓN PARA EL APOYO A LA TOMA DE DECISIONES

Debilidades en la calidad de la información para la toma de decisiones

2.1. Se encontró que la DGME cuenta con sistemas de información que han cumplido su vida útil y que presentan problemas de calidad de la información. También se evidencian problemas de integración de los sistemas, donde las principales aplicaciones no comparten información que es importante para la toma de decisiones.

2.2. Además, algunos documentos migratorios como el salvoconducto y documentos de viaje para personas extranjeras se confeccionan manualmente y su control es a través de hojas de cálculo, sin ningún nivel de integración con los sistemas computacionales.

2.3. El equipo de auditoría realizó un sondeo mediante el cual se consultó a las jefaturas de las áreas usuarias de la DGME respecto a la calidad de los sistemas de información. Su mayor preocupación se centró en las debilidades de los reportes para toma de decisiones.

2.4. GTI suministra un inventario de al menos 250 reportes preestablecidos, los cuales no son conocidos por todos los usuarios, quienes en vez de buscar en las listas de los reportes ya creados, prefieren solicitar la información de nuevo a GTI, a pesar de que en muchos casos deban esperar una o dos semanas para obtener la información, dependiendo del nivel de trabajo que tenga el personal de esa Unidad. De acuerdo con el sondeo mencionado, los usuarios consideran que un 35% de los informes para toma de decisiones se obtienen de esta manera.

2.5. La generación de requerimientos nuevos de información para toma de decisiones no está en manos de los usuarios y, según la opinión de las jefaturas, un 43% de los reportes prediseñados no cumplen con la capacidad para parametrizar o definir características de la información a analizar.

2.6. En el caso del Despacho de la Directora de la DGME, este solicita la información para la toma de decisiones a la Unidad de Planificación Institucional, quien, según el sondeo realizado, es el mayor demandante de informes hacia GTI, con un 40% de los requerimientos, seguido de Operaciones con un 28%. Del total de los informes, los usuarios consideran que, en un 50% de los casos, la información suministrada es insuficiente.

2.7. De acuerdo con la consulta realizada a las jefaturas de la DGME, existen oportunidades de mejora importantes en materia de calidad de información para la toma de decisiones, tanto estratégicas como operativas. Los usuarios apuntan factores como la falta de oportunidad (22% de los casos); claridad (9%); disponibilidad (27% de los procesos requieren de esfuerzos adicionales para procesar información); y flexibilidad (46%); así como, dificultades para la parametrización (43%) y una presentación que no es la adecuada para el usuario (27%).

2.8. Uno de los factores que hacen más valiosa la información en los procesos de toma de decisiones, es la disponibilidad para el usuario que la requiere en el momento preciso. Los usuarios de la DGME consideran que un 39% de los informes no se entregan a tiempo, y para hacer más sensible esta situación, un 42% de los informes no satisfacen al usuario final.

2.9. Las debilidades enunciadas se contraponen a lo estipulado en la Ley General de Control Interno, la cual, en su artículo 8 indica, entre otras cosas, que se debe garantizar la "confiabilidad y oportunidad de la información" y "garantizar la eficiencia y eficacia de las operaciones".

2.10. Por su parte, en el artículo 16 de las Normas Técnicas de Control Interno para el Sector Público se establece que los sistemas de información deben "contar con procesos que permitan identificar y registrar información confiable, relevante, pertinente y oportuna; asimismo, que la información sea comunicada a la administración activa que la necesite, en la forma y dentro del plazo requeridos para el cumplimiento adecuado de sus responsabilidades, incluidas las de control interno".

2.11. Además, en el inciso 5.8 de esta normativa se indica que "el jerarca y los titulares subordinados, según sus competencias, deben disponer los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información".

2.12. Por su parte, las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), en su aparte 1.1 establece que "el jerarca debe traducir sus aspiraciones en materia de TI en prácticas cotidianas de la organización, mediante un proceso continuo de promulgación y divulgación de un marco estratégico constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido".

2.13. Además, este cuerpo normativo, en el punto 1.2 establece que "la organización debe generar los productos y servicios de TI de conformidad con los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo".

2.14. Por su parte, también la norma 2.2 estipula que "la organización debe optimizar la integración, uso y estandarización de sus sistemas de información de manera que se identifique, capture y comunique, en forma completa, exacta y oportuna, sólo la información que sus procesos requieren".

2.15. En cuanto a las buenas prácticas incluidas en COBIT 5[1], estas indican, en su proceso APO02 "Gestionar la Estrategia" que se deben "alinear los planes estratégicos de TI con los objetivos del negocio. Comunicar claramente los objetivos y las cuentas asociadas para que sean comprendidos por todos, con la identificación de las opciones estratégicas de TI, estructurados e integrados con los planes de negocio".

[1] COBIT 5 es el marco de trabajo para el gobierno y la gestión de las TI en las organizaciones desarrollado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA por sus siglas en inglés).

2.16. Este mismo proceso de COBIT 5, en su práctica de gestión APO02.05 (Definir el plan estratégico y la hoja de ruta) especifica que se debe "crear un plan estratégico que defina, en cooperación con las partes interesadas más relevantes, cómo los objetivos de TI contribuirán a los objetivos estratégicos de la empresa. Incluyendo cómo TI apoyará el programa aprobado de inversiones, los procesos de negocio, servicios y activos de TI. Orientar las tecnologías para definir las iniciativas que se requieren para cerrar las diferencias, la estrategia de abastecimiento y las medidas que se utilizarán para supervisar el logro de los objetivos, para dar prioridad a las iniciativas y combinarlas en una hoja de ruta a alto nivel".

2.17. Además, en su proceso APO03 "Administrar la Arquitectura Empresarial" recomienda que se debe "establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Definir los requisitos para la taxonomía, las normas, las directrices, los procedimientos, las plantillas y las herramientas y proporcionar un vínculo para estos componentes. Mejorar la adecuación, aumentar la agilidad, mejorar la calidad de la información y generar ahorros de costes potenciales mediante iniciativas tales como la reutilización de bloques de componentes para los procesos de construcción".

2.18. En cuanto a la gestión de la calidad, estas buenas prácticas indican en su proceso APO11 "Gestionar la Calidad", en la práctica de gestión 01, que se debe "establecer un sistema de gestión de la calidad (…) que proporcione una aproximación a la gestión de la calidad para la información, la tecnología y los procesos de negocio que sea continua, estandarizada, formal y que esté alineada con los requerimientos del negocio y con la gestión de la calidad a nivel corporativo". Asimismo, la práctica de gestión APO11.03 (Enfocar la gestión de la calidad en los clientes) indica que se debe "enfocar la gestión de la calidad en los clientes, mediante la determinación de sus necesidades y asegurar el alineamiento con las prácticas de gestión de calidad".

2.19. El mandato de Ley y el entorno en que se encuentra la DGME hacen que ésta requiera de sistemas de información ágiles que respalden la toma de decisiones a todo nivel para garantizar un control migratorio eficaz y el alineamiento de las tecnologías de información con la estrategia institucional.

2.20. En este sentido, se puede establecer que las debilidades apuntadas obedecen, primariamente, a la ausencia de un marco estratégico de TI que alinee los esfuerzos de GTI con la estrategia institucional, de manera oportuna y continua, para satisfacer las necesidades de los usuarios y apoyar la toma de decisiones estratégicas de forma efectiva. Esto, por cuanto la DGME no cuenta con un Plan Estratégico de Tecnologías de Información (PETI). GTI informa que se está confeccionando uno como respuesta al Plan Estratégico Institucional (PEI) (este último abarca el período 2015-2019). Esperan que el PETI esté concluido a finales de este año, con lo que empezaría a regir en el año 2018; al menos tres años después del establecimiento del PEI.

2.21. Además, se une a estas debilidades estratégicas la inexistencia de una arquitectura de información que soporte la integración, uso y estandarización de los sistemas de información, que contribuya a la calidad de la información para una toma de decisiones ágil, oportuna y confiable.

2.22. Por otra parte, GTI tampoco cuenta con un sistema de gestión de la calidad de la información que garantice la confiabilidad del contenido de las bases de datos, y además que brinde garantía razonable de oportunidad, completitud, disponibilidad, claridad e integración de la información, para el apoyo a la toma de decisiones en un entorno altamente riesgoso y cambiante.

2.23. Además de las situaciones mencionadas sobre integración y calidad de la información, subsiste la problemática de la oportunidad de los informes para la toma de decisiones estratégicas; lo cual se debe a la ausencia de herramientas que permitan que los usuarios generen sus propios reportes y así agilizar su producción, liberar recursos altamente costosos de GTI y contar con información más exacta y completa, en menos tiempo, para tomar mejores decisiones.

2.24. La administración efectiva de los flujos migratorios por parte de la DGME representa un importante desafío; los puestos fronterizos son la puerta de entrada y salida al país y por ello requieren de un control migratorio eficaz, que se base en información de calidad que sirva de respaldo para la toma de decisiones ágiles y oportunas.

2.25. Las debilidades mencionadas no permiten generar esa información requerida, alineada a las necesidades de la institución, en los tiempos óptimos para que las decisiones necesarias sean tomadas en aras del efectivo control migratorio que garantice un apoyo contundente a la seguridad ciudadana del país.

SEGURIDAD DE LA INFORMACIÓN

Debilidades en la gestión de permisos a usuarios para el acceso a los sistemas institucionales

2.26. En tecnologías de información, un alto porcentaje de los incidentes de seguridad son atribuidos a empleados o a exempleados que aprovechan vulnerabilidades y violentan la seguridad de la organización; en su mayoría se valen de atribuciones asignadas en permisos (roles) que les facilitan acceder a información que ya no debería estar bajo su control.

2.27. En la DGME existe un riesgo alto de manipulación inadecuada de la información al presentarse un retraso en los ajustes a los permisos de acceso, asignados por roles, a funcionarios que cambian su condición o ubicación laboral o dejan de laborar para la institución, por cuanto continúan activas credenciales que deberían ser canceladas o cambiadas en forma inmediata, de acuerdo con la nueva situación funcional del colaborador.

2.28. Esta situación se agrava dada la sensibilidad de la información y de los procesos que lleva a cabo la DGME, muchos de los cuales son de sumo interés para grupos de crimen organizado o personas inescrupulosas.

2.29. Al respecto, GTI manifiesta que ha realizado esfuerzos para obtener esta información de cambio de situación laboral de manera ágil y oportuna, solicitando colaboración a la unidad de Recursos Humanos pero que aún espera respuesta de un oficio girado en este sentido en el año 2013.

2.30. El control de privilegios para el acceso a los sistemas de información es una actividad de Control Interno básica, mediante la cual se debe garantizar razonablemente que los usuarios solo puedan acceder a la información estrictamente necesaria para el desempeño de sus funciones, así como la trazabilidad de las acciones de los funcionarios en su interacción con los sistemas de información. De acuerdo con las Normas de control interno para el Sector Público (N-2-2009-CO-DFOE), el punto 5.8 establece que "el jerarca y los titulares subordinados, según sus competencias, deben disponer los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación, la seguridad y **una clara asignación de responsabilidades y administración de los niveles de acceso a la información y datos sensibles**, así como la garantía de confidencialidad de la información que ostente ese carácter" (el destacado no es del original).

2.31. Por su parte, las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), en su punto 1.4 indican 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: (…) **El control de acceso**. (…) Además debe establecer las medidas de seguridad relacionadas con: (…) **La terminación normal de contratos, su rescisión o resolución**" (el destacado no es del original).

2.32. 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 bajo el principio de necesidad de saber o menor privilegio. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones. 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".

2.33. 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" (el destacado no es del original).

2.34. También COBIT 5 menciona, en la práctica de gestión DSS06.03 (Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización) que se deben "gestionar los roles de negocio, responsabilidades, niveles de autoridad y segregación de tareas necesarias para apoyar los objetivos del proceso de negocio. Autorizar el acceso a cualquier activo de información relativo a los procesos de información del negocio, incluyendo aquellos bajo la custodia del negocio, de TI y de terceras partes. Esto asegura que el negocio sabe dónde están los datos y quien los está manejando en su nombre". Para esta práctica de gestión, establece que se deben llevar a cabo, entre otras, las siguientes actividades: "asignar roles y responsabilidades sobre la base de la descripción aprobada de puestos y actividades de procesos de negocio asignadas. Asignar derechos de acceso y privilegios solo 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**" (el destacado no es del original).

2.35. Por último, la Norma ISO 27002 "Código de prácticas para la gestión de la seguridad de la información", también nos indica, en su aparte 8.3.3 que "los derechos de acceso de todo empleado, contratista o usuario de terceras partes a información e instalaciones de procesamiento de información **deberían ser removidos como consecuencia de la desvinculación de su empleo, contrato o acuerdo, o ajustado cuando cambia**" (el destacado no es del original).

2.36. La debilidad de actualización oportuna de permisos de acceso a los sistemas (roles) mencionada, se presenta por la falta de un procedimiento formal, aprobado, comunicado y vinculante que garantice que la unidad de Recursos Humanos, y las demás unidades usuarias, informen de manera inmediata a GTI cualquier cambio en la relación laboral con los funcionarios.

2.37. La modificación de los niveles de acceso de los funcionarios, cuando corresponda, debe ser realizada de manera inmediata para garantizar que la información institucional a todo nivel está protegida contra accesos no autorizados de personal que ha cambiado sus funciones o que ha abandonado la organización.

2.38. Como ya se mencionó, la mayor parte de los problemas de manejos indebidos de información, en las organizaciones, provienen de personal interno, ya sea por dolo o por descuido, y la información y procesos de la DGME son sensibles a intereses externos que pueden pretender aprovechar estas vulnerabilidades en su beneficio para insertarse en nuestro país y cometer ilícitos, con el correspondiente efecto negativo para la seguridad ciudadana.

Documentos del plan de continuidad de negocio incompletos

2.39. Las actividades que lleva a cabo la DGME para el control de ingreso y salida de personas por los diferentes puestos migratorios, así como las labores que presta para evitar actos delictivos que involucren flujos migratorios de personas que permanezcan en el territorio nacional o que pretendan abandonarlo, son funciones que requieren una disponibilidad continua de información, todos los días del año y 24 horas al día, dado que las labores de varios de estos puestos de ingreso y egreso son continuas.

2.40. En este sentido, la DGME cuenta con varios documentos que son parte de la planificación para la continuidad de negocio, entre los cuales se pueden mencionar: el análisis de impacto de negocio (BIA por sus siglas en inglés), el cual define la criticidad de las funciones que se llevan a cabo en la institución; el plan de recuperación de desastres (DRP por sus siglas en inglés), que indica las actividades que se deben llevar a cabo para recuperar las operaciones de la institución luego de que se presente un evento que involucre una suspensión de servicios informáticos; y el plan de continuidad de negocio (BCP por sus siglas en inglés) que incluye los procedimientos que deben llevarse a cabo durante una interrupción de servicios para garantizar la supervivencia de la organización, operando al menos con las funciones definidas como críticas, para brindar un servicio mínimo a los usuarios.

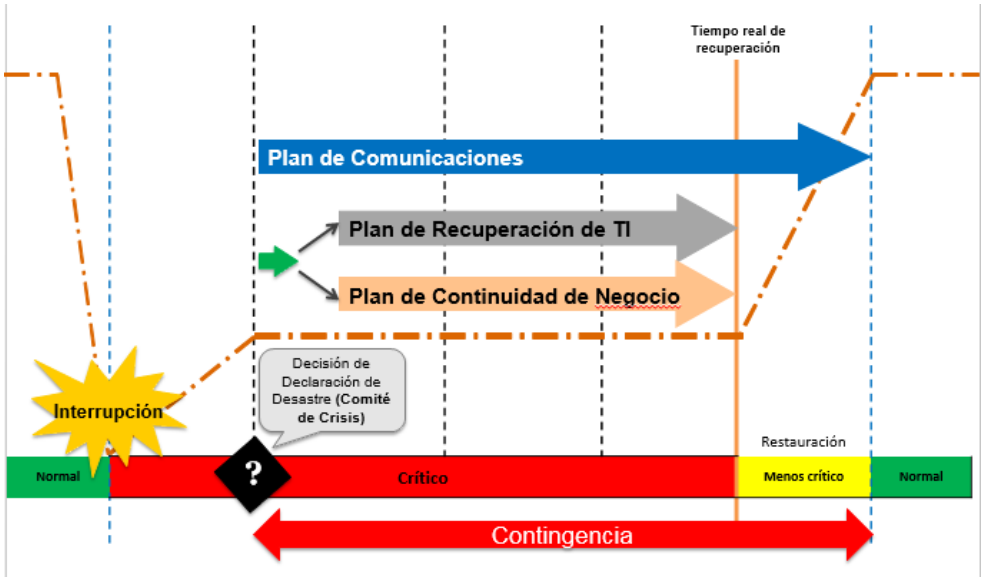
2.41. De esta forma, en el análisis de impacto de negocio de la DGME, no se incluyeron los puntos objetivos de recuperación[2] para cada función crítica, información relevante para la definición de los controles y procedimientos que se deben establecer para minimizar la pérdida de información en caso de eventos adversos.

2.42. Por su parte, al revisar el documento del DRP, llama la atención la condición de "pendiente" para la designación de la persona que debe desempeñar el papel de "líder de recuperación ante desastres", que sería la persona encargada, entre otras funciones, de la recuperación general de la infraestructura, los sistemas y aplicaciones de la DGME durante una interrupción, incluyendo la ejecución misma del DRP, también sería el encargado de coordinar las pruebas y mantenimiento del DRP y actualizarlo de acuerdo con cambios en el entorno de TI.

[2] RPO por sus siglas en inglés, es definido en la Norma ISO 22301 como el punto en el cual la información utilizada por una actividad debe ser restaurada para permitir la reanudación de la operación, también se puede denominar como "pérdida máxima de datos".

2.43. Por otra parte, tal como se muestra en la figura N.° 1, luego de una interrupción que amerite la ejecución del DRP, mientras se reestablecen los servicios, la institución debe operar bajo los protocolos establecidos en el BCP para garantizar la atención de los usuarios en los servicios considerados críticos. Luego de revisar el BCP, estos protocolos son inexistentes y este plan se limita a describir las funciones normales de la institución y a indicar que en caso de suspensión de servicios informáticos, se consulte a la jefatura correspondiente, lo que no garantiza la continuidad de las operaciones a ningún nivel.

Figura N.° 1
Proceso de activación de los planes



Fuente: DRP de la DGME.

2.44. Además, se indica en el BCP que existen funciones que no cuentan con un plan de contingencia y que son “las más utilizadas por los usuarios”, dentro de las cuales se enlistan los trámites de pasaportes, emisión y renovación del Documento de Identidad Migratoria para Extranjeros (DIMEX), estudio y valoración de solicitudes de permanencia legal en Costa Rica, entre otros, por lo que en el documento se recomienda “tomar las acciones necesarias para establecer procedimientos de recuperación tecnológicos, esto con el fin de impactar en el menor nivel posible la imagen y reputación de la DGME”, pero no propone cómo operar en contingencia, y en caso de una falla prolongada, estos servicios no se prestarían del todo.

2.45. La ausencia de los protocolos de acción durante una interrupción de los servicios tecnológicos, toma mayor relevancia al revisar lo indicado en el BIA con respecto a los tiempos máximos de recuperación, donde muchas de las funciones críticas cuentan con un tiempo objetivo de recuperación (RTO)[3] que no puede ser mayor a una hora, y otra cantidad importante indica que su RTO debe ser inferior a cuatro horas, lo que revela que tiempos superiores a estos son inaceptables para la operación de la organización. No obstante, al revisar los documentos que respaldan el DRP se puede visualizar que los tiempos requeridos para reconstruir los servicios de los equipos principales de la institución, desde los respaldos, superan por mucho los tiempos establecidos en el BIA. Se indica que el contrato con el proveedor estipula 16 horas como máximo para iniciar la reparación, para luego llevar a cabo tareas como solicitar cintas de respaldo, instalación y configuración de los equipos, restauración del respaldo, entre otros, los cuales suman muchas más horas que las definidas como aceptables en el BIA. Recordemos que el DRP "está diseñado para ayudar a minimizar el efecto de un desastre, asegurando la restauración de procedimientos esenciales dentro de los RTO establecidos por el BIA" (como lo indica el mismo documento confeccionado por la DGME).

2.46. Por último, al revisar los procedimientos de recuperación ante desastres, anexos al DRP, se observa que en su mayoría están incompletos, por ejemplo, el procedimiento de recuperación de servidores no tiene indicados todos los encargados de las áreas involucradas (de cuatro áreas solamente una presenta esta información); asimismo, el cuadro de proveedores cuenta con tres columnas completamente en blanco, a saber: tiempo de respuesta por contrato, número de contrato y equipos bajo el contrato. Por su parte, la tabla de descripción de los equipos no cuenta con nombres de los archivos de recuperación, números de activo ni servicios que soporta cada servidor. Algunos otros de estos procedimientos, no cuentan con los números de teléfono de los responsables del proceso y ninguno cuenta con hoja de control de cambios donde se indique el nivel de actualización del documento.

2.47. Se une a esta problemática que la DGME no cuenta con personal disponible para cubrir las contingencias que podrían ocurrir fuera del horario normal de la institución, con lo cual, al presentarse un incidente fuera de horas laborales su atención iniciaría al día hábil siguiente, al iniciar labores en horario normal.

2.48. Las situaciones enumeradas son contrarias a lo que indican las Normas de control interno para el Sector Público (N-2-2009-CO-DFOE), cuya norma 5.9 estipula que "deben instaurarse los mecanismos y procedimientos manuales que permitan garantizar razonablemente la operación continua y correcta de los sistemas de información".

[3]RTO por sus siglas en inglés, es definido en la Norma ISO 22301 como el período de tiempo después de un incidente en el que: el producto o servicio debe ser reanudado, o la actividad debe reanudarse o los recursos deben ser recuperados. Para los productos, servicios y actividades, el tiempo objetivo de recuperación debe ser menor que el tiempo que tomaría para los efectos adversos que pudieran surgir como consecuencia de no proporcionar un producto/servicio o la realización de una actividad para convertirse en inaceptable.

2.49. Por su parte, las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), en la norma 1.4 establece 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).

2.50. Adicionalmente, esta norma técnica señala, en su punto 1.4.7, 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".

2.51. Las buenas prácticas establecidas en el marco de COBIT 5, 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 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).

2.52. Asimismo, 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".

2.53. También, 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.

2.54. Por último, este marco de buenas prácticas, en su práctica de gestión DSS04.04 (Ejercitar, probar y revisar el plan de continuidad) establece la necesidad de "probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcionará, en el tiempo, como se espera".

2.55. Por su parte, la Norma ISO 22301 (Seguridad de la Sociedad. Sistemas de gestión de continuidad del negocio. Requisitos) define la continuidad del negocio como la "capacidad de la organización para continuar suministrando productos o servicios a niveles predefinidos aceptables, posterior a un incidente disruptivo". También define la gestión de la continuidad del negocio como el "proceso integral de gestión que identifica las amenazas potenciales para una organización y los posibles impactos para las operaciones del negocio de estas amenazas, en caso de que ocurran y proporciona un marco para la construcción de la resiliencia de la organización con la capacidad de una respuesta efectiva que salvaguarde los intereses de sus partes interesadas clave, así como su reputación, marca y actividades que crean valor". Por último, define el plan de continuidad del negocio como los "procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel pre-definido de operación después de una interrupción".

2.56. Esta misma norma ISO especifica que se deben establecer e implementar procedimientos de continuidad del negocio "para gestionar un incidente disruptivo y continuar con sus actividades basadas en los objetivos de recuperación identificadas en el análisis de impacto al negocio. La organización debe documentar los procedimientos (incluidos los acuerdos necesarios) para asegurar la continuidad de actividades y la gestión de un incidente disruptivo. Los procedimientos deben: a) establecer un protocolo de comunicaciones interno y externo adecuado, b) ser específicos con respecto a las medidas inmediatas que deben tomarse durante una interrupción, c) ser flexibles para responder a amenazas imprevistas y las cambiantes condiciones internas y externas, d) centrarse en el impacto de los eventos que podrían potencialmente interrumpir las operaciones, e) ser desarrollados con base a los supuestos establecidos y el análisis de las interdependencias, f) ser eficaz en la reducción de sus consecuencias a través de la aplicación de estrategias apropiadas de mitigación".

2.57. Como indica la normativa, el análisis de impacto de negocio debe basarse en un análisis de los riesgos relevantes y debe servir de insumo para la confección del plan de continuidad y el plan de recuperación de desastres. Las debilidades anotadas se deben a que no existe evidencia ni referencia alguna a que haya sido confeccionado de esta manera, no se cuenta con un análisis de riesgos que lo respalde, ni se hace mención al mismo en ningún aparte; adicionalmente, los documentos que componen estos planes están incompletos o no corresponden los parámetros de unos con los otros; por ejemplo, la cantidad de horas del tiempo de recuperación objetivo contra el tiempo real para recuperar un servidor no son congruentes, no se cuenta con procedimientos de recuperación en sitios alternos luego de un desastre de niveles superiores, tampoco se especifica la disponibilidad de personal que atienda los incidentes las 24 horas del día.

2.58. Los documentos que conforman el plan de continuidad de negocio son producto de una contratación externa, y no han sido validados por el área técnica respectiva dado que fueron producto de una contratación dirigida por la Unidad de Planificación Institucional.

2.59. Las condiciones actuales de los diferentes documentos que conforman el plan de continuidad de negocio de la DGME, no garantizan la ejecución de las funciones críticas, en condiciones de operación en contingencia por efecto de eventos adversos que interrumpan los servicios tecnológicos de la institución; esto acarrearía suspensión de los servicios críticos a los usuarios de la DGME con los problemas directos sobre la entrada y salida de personas del país, confección y entrega de documentos de identificación, visas y otros, lo cual podría redundar en movimientos migratorios anómalos y contrarios al ordenamiento jurídico y a la seguridad ciudadana.

Problemas de seguridad por disparidad de versiones de software y uso de programas descontinuados

2.60. Las versiones obsoletas de aplicaciones computacionales, principalmente sistemas operativos, presentan vulnerabilidades que se pueden explotar y que acarrean problemas de seguridad de gran magnitud; similar situación se presenta con programas informáticos que no cuenten con sus últimas versiones y actualizaciones.

2.61. La GTI de la DGME mantiene un alto riesgo de operación y de atrasos en la recuperación de servicios ante fallas, debido a la diversidad de versiones de sistemas operativos y en algunos casos obsolescencia de estos, esto último puede implicar no contar con respaldo del fabricante, tanto para servidores como para estaciones de trabajo.

2.62. Los problemas de estandarización, en cuanto a versiones de un mismo sistema operativo, complican la administración de actualizaciones, algunas de las cuales se presentan a veces como cambios de emergencia ante el descubrimiento de vulnerabilidades del software. La administración de la aplicación de estos cambios, a diferentes versiones del mismo producto, puede llevar a errores y a interrupción del servicio.

2.63. Por otra parte, GTI, en su Guía de requerimientos de seguridad informática para sistemas instalados, indica que debe existir un ambiente de pruebas, configurado y probado, para la aplicación de parches de seguridad de software; ambiente de pruebas que no existe a la fecha.

2.64. A lo anterior se une la existencia de listados desactualizados de equipos y sus respectivas licencias, los cuales son la base para la recuperación de la infraestructura tecnológica en caso de una interrupción de servicios debido a fallas o daños en equipos.

2.65. El problema de versiones disímiles de sistemas operativos, y de software en general, es tratado por la Unidad de Seguridad de Información de la DGME, en el Informe final del proyecto “Hardening Servers & PC”, de marzo 2017, donde se indica que es muy complejo hacer un perfil de seguridad a nivel de aplicaciones y puertos cuando se tienen sistemas operativos heterogéneos y fuera de soporte técnico. Asimismo, en la Guía de requerimientos de seguridad informática para sistemas instalados de la DGME, se indica que se debe instalar la última versión liberada estable en su momento, con las actualizaciones de seguridad que el proveedor indique, y que debe existir un ambiente de pruebas configurado y probado para la aplicación de actualizaciones de seguridad de software.

2.66. Estas versiones de software, así como toda la infraestructura que soporte las aplicaciones, deben estar acordes con la arquitectura de información de la organización, tal como lo establece la norma 3.3 “Implementación de infraestructura tecnológica”, de las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE).

2.67. Asimismo, este cuerpo normativo, en su punto 4.2 indica que “la organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe: a. Establecer y documentar los procedimientos y las responsabilidades asociados con la operación de la plataforma. b. Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas. c. Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas. d. Controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (hardware y software), custodiar adecuadamente las licencias de software y realizar verificaciones físicas periódicas. e. Controlar la ejecución de los trabajos mediante su programación, supervisión y registro. f. Mantener separados y controlados los ambientes de desarrollo y producción”.

2.68. Para ampliar la necesidad de mantener ambientes separados de prueba y producción, las mejores prácticas establecidas en COBIT 5, específicamente la práctica de gestión BAI07.04 indica que se debe “definir y establecer un entorno seguro de pruebas que sea representativo del proceso de negocio y entorno de operaciones de TI planeados, en cuanto a rendimiento y capacidad, seguridad, controles internos, prácticas de operación, calidad de los datos y requisitos de privacidad y carga de trabajo”.

2.69. Por su parte, en cuanto a los equipos de usuario final, las buenas prácticas de COBIT 5 establecen, en la práctica de gestión DSS05.03 que se debe “asegurar que los puestos de usuario final (es decir, portátil, equipo sobremesa, servidor y otros dispositivos y software móviles y de red) están asegurados a un nivel que es igual o mayor al definido en los requerimientos de seguridad de la información procesada, almacenada o transmitida” para lo cual se deben “configurar los sistemas operativos de forma segura”.

2.70. También, como ya se dijo, COBIT 5 recomienda gestionar la arquitectura de información (proceso APO03 ya citado), al indicar que se debe “establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo”.

2.71. Por último, COBIT 5 también indica que la organización debe “administrar las licencias de software de forma que se mantenga el número óptimo de licencias para soportar los requerimientos de negocio y el número de licencias en propiedad sea suficiente para cubrir el software instalado y en uso” (BAI09.05) para lo cual debe “de forma regular, considerar si se puede obtenerse [*sic*] un mejor valor mediante la actualización de productos y licencias asociadas”.

2.72. La principal causa de los problemas de diversas versiones del mismo software, así como su actualización y control y la existencia de aplicaciones obsoletas y sin respaldo del fabricante, residen en la falta de un modelo de arquitectura de información completo y actualizado de forma permanente, que sirva como herramienta para realizar una gestión eficaz de la plataforma tecnológica de la DGME.

2.73. Adicionalmente, la desactualización de los documentos de respaldo a los planes de recuperación de desastres y de continuidad de negocio obedece a la falta de responsables por procedimiento, y de directrices que indiquen la obligatoriedad de mantener estos documentos actualizados cada vez que se generan cambios en cualquier pieza de la infraestructura tecnológica.

2.74. Indica la Administración que las versiones de software se han mantenido así, en algunos casos, por tratarse de equipos muy viejos, en otros por falta de pruebas para ver si los equipos soportan las nuevas versiones, y en otras por falta de recursos o personal; lo que refleja la falta de procedimientos y responsables que se aseguren de minimizar los riesgos inherentes que se presentan al mantener estas prácticas de manejo de software que es crítico para la institución, y la falta de un ambiente de pruebas que garantice la correcta aplicación de estas actualizaciones minimizando el riesgo de interrupciones del servicio.

2.75. Como resultado, la carencia de un modelo de arquitectura de información, impide que los recursos de TI se estén gestionando de manera eficiente y eficaz, alineados a los objetivos estratégicos, tanto de GTI como institucionales, lo que redunda en un uso limitado de la información para la toma de decisiones.

2.76. Adicionalmente, el uso de versiones obsoletas y descontinuadas de sistemas operativos, tanto para servidores como para equipos de escritorio, que ya no cuentan con respaldo por parte del fabricante, trae consigo el riesgo de que se presenten brechas de seguridad en estos productos y no contar con la actualización oportuna, lo que llevaría a la permanencia de la vulnerabilidad y la exposición a ataques o interrupciones de los servicios y su correspondiente implicación en la toma de decisiones institucional. Esto se agrava al no contar con un ambiente separado, donde se puedan realizar pruebas efectivas de las actualizaciones que se presenten al software institucional.

2.77. Por último, la falta de actualización de los documentos de descripción de los equipos y de los procedimientos que son base para la recuperación en caso de interrupción de servicios tecnológicos, puede desencadenar mayores tiempos de recuperación y por ende mayores tiempos de interrupción de los servicios a los usuarios de la DGME.

3. CONCLUSIONES

3.1. La DGME es la institución encargada del control migratorio en el país, responsable de recomendar y ejecutar la Política Migratoria Integral que dicta el Poder Ejecutivo, que forma parte sustancial del orden público y la seguridad nacional, procurando la promoción de los derechos humanos y garantías constitucionales de las personas migrantes y que su aporte se convierta en un elemento para el desarrollo del país; sin menoscabo de los controles de ingreso de personas extranjeras al territorio nacional, su permanencia en él, así como su egreso, en concordancia con la seguridad pública y los mejores intereses del país.

3.2. Para cumplir con todas esas funciones, la DGME requiere información veraz, ágil y oportuna que le permita tomar las decisiones apropiadas en el momento preciso; información que debe recibir y procesar de sistemas modernos, integrados, consolidados y robustos, que garanticen la calidad y seguridad de la información.

3.3. En el presente informe se ha establecido que la información contenida en los sistemas de la DGME, carece de los niveles de calidad que requieren los usuarios para el desempeño efectivo y oportuno de sus funciones, y para la confección de las proyecciones estratégicas que se deben llevar a cabo en aras de la seguridad ciudadana y de un efectivo control de los flujos migratorios.

3.4. Por otra parte, a pesar de que la administración cuenta con un proceso de TI que se encarga de la seguridad de la información, se han encontrado vulnerabilidades que pueden llegar a exponer información sensible a personas inescrupulosas que pueden pretender hacer uso ilegítimo de la misma para actividades delictivas, así como incrementar el riesgo de pérdida o corrupción de información por dolo o impericia; además de las amenazas que atentan contra la continuidad de los servicios y controles migratorios que presta la DGME a la sociedad costarricense al no contarse con un efectivo plan de continuidad de negocio.

3.5. Es urgente que en el corto plazo, se tomen las medidas necesarias que contribuyan a mitigar las situaciones descritas en este informe, esto aún y cuando la Administración indica que se tienen en proyecto dos nuevos sistemas, los cuales se encuentran en etapas previas a su ejecución y constituyen una expectativa a futuro, que podrían solucionar algunas de las deficiencias apuntadas en este informe.

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 04 de enero de 2016.

4.3. El 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 SEÑORA LILLIAM JARQUÍN MORALES EN SU CALIDAD DE PRESIDENTA DE LA JUNTA ADMINISTRATIVA DE LA DIRECCIÓN GENERAL DE MIGRACIÓN Y EXTRANJERÍA, O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.4. Elaborar, aprobar y divulgar el Plan Estratégico de Tecnologías de Información, el cual deberá estar alineado con la estrategia institucional. Enviar a la Contraloría General, al 30 de marzo de 2018 una certificación del acuerdo emitido por la Junta Administrativa mediante el cual se aprueba el nuevo Plan Estratégico de Tecnologías de Información y que se encuentra alineado con la estrategia institucional para respaldar la toma de decisiones. Ver párrafos del 2.1 al 2.25 de este informe.

4.5. Establecer lineamientos para que cuando se emitan modificaciones al Plan Estratégico Institucional, el Plan Estratégico de Tecnologías de Información se mantenga alineado con la estrategia institucional. Enviar a la Contraloría General, a más tardar el 30 de marzo de 2018, una certificación que acredite el establecimiento y comunicación de los lineamientos solicitados. Ver párrafos del 2.1 al 2.25 de este informe.

4.6. Revisar, ajustar y oficializar el plan de continuidad de negocio y alinearlo con el plan de recuperación de desastres, tomando en cuenta el análisis de impacto de negocio basado en un análisis completo de los riesgos relevantes de la institución; que incluya las acciones efectivas a ejecutar en caso de incidentes que resulten en suspensión de los servicios informáticos en las áreas críticas institucionales; para garantizar razonablemente y dentro de parámetros realistas la continuidad de los servicios que brinda la Dirección General de Migración y Extranjería; a fin de salvaguardar la integridad del territorio nacional y el apego al ordenamiento jurídico. Enviar a la Contraloría General, a más tardar el 30 de abril de 2018, una certificación del acuerdo emitido por la Junta Administrativa mediante el cual se aprueba y oficializa el plan de continuidad de negocio; y a más tardar el 31 de julio de 2018 una certificación que acredite la realización de pruebas que garanticen que el plan minimizará cualquier impacto producto de incidentes que involucren suspensión de servicios tecnológicos. Ver párrafos del 2.39 al 2.59 de este informe.

4.7. Confeccionar y aprobar un modelo de arquitectura de información que apoye la integración y calidad de la información que se mantiene en los sistemas de información institucionales, y los procedimientos para mantenerlo actualizado. Enviar a la Contraloría General, a más tardar el 29 de junio de 2018, una certificación del acuerdo emitido por la Junta Administrativa mediante el cual se acredita la aprobación del modelo de arquitectura de información y de los procedimientos que garanticen su actualización permanente. Ver párrafos del 2.1 al 2.25 de este informe.

A LA SEÑORA GISELA YOCKCHEN MORA EN SU CALIDAD DE DIRECTORA GENERAL DE MIGRACIÓN Y EXTRANJERÍA, O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.8. Definir, aprobar e implementar un procedimiento de carácter obligatorio mediante el cual las unidades usuarias, incluido el departamento de Recursos Humanos, informen a Gestión de Tecnologías de Información en el momento en que se produzca cualquier movimiento de personal que involucre la confección, modificación o eliminación de privilegios para acceder a la información institucional; así como la obligatoriedad de que Gestión de Tecnologías de Información realice las modificaciones respectivas de forma inmediata. Enviar a la Contraloría General, a más tardar el 28 de febrero de 2018, una certificación que acredite la definición, aprobación, divulgación e implementación del respectivo procedimiento. Ver párrafos del 2.26 al 2.38 de este informe.

4.9. Establecer mecanismos de control para velar por el estricto cumplimiento del procedimiento de actualización de permisos de acceso a la información institucional, con el propósito de que, en los casos que se presenten desviaciones, se tomen las acciones correctivas que correspondan. Enviar a la Contraloría General, a más tardar el 30 de abril de 2018, una certificación que acredite la definición e implementación de estos mecanismos de control. Ver párrafos del 2.26 al 2.38 de este informe.

A LA SEÑORA JENNY GAMBOA RODRÍGUEZ EN SU CALIDAD DE GESTORA DE TECNOLOGÍAS DE INFORMACIÓN, O A QUIEN EN SU LUGAR OCUPE EL CARGO

4.10. Elaborar e implementar un sistema de gestión de calidad de la información, que garantice razonablemente la verificación de los atributos de la información y su mejora continua para la toma de decisiones institucionales. Enviar a la Contraloría General, a más tardar el 31 de mayo de 2018, una certificación que acredite la elaboración del sistema de gestión de la calidad de la información, y al 31 de julio de 2018, una certificación que acredite la operación efectiva del sistema de gestión de la calidad de la información. Ver párrafos del 2.1 al 2.25 de este informe.

4.11. Elaborar e implementar, a nivel institucional, herramientas para que los usuarios finales puedan extraer, de las bases de datos institucionales, la información relevante acorde con sus funciones, con el propósito de que puedan generar sus propios informes para la toma de decisiones de manera oportuna. Enviar a la Contraloría General, a más tardar el 31 de julio de 2018, una certificación que acredite la implementación de las herramientas que permitan la generación de informes para la toma de decisiones por parte de los usuarios finales. Ver párrafos del 2.1 al 2.25 de este informe.

4.12. Establecer e implementar un procedimiento para la utilización de un ambiente de pruebas permanente para las actualizaciones de software, así como realizar las actualizaciones y migraciones de los sistemas operativos que procedan, para minimizar la exposición a vulnerabilidades procedentes de software desactualizado, obsoleto o sin respaldo del fabricante. Enviar a la Contraloría General, a más tardar el 30 de marzo de 2018, una certificación que acredite el establecimiento del procedimiento solicitado; y al 31 de mayo de 2018 una certificación que acredite la implementación del procedimiento para la constitución del ambiente de pruebas. Ver párrafos del 2.60 al 2.77 de este informe.

4.13. Definir e implementar procedimientos para mantener actualizados, en forma permanente, todos los documentos y software que respaldan la gestión de tecnologías de información a todo nivel. Este procedimiento debe contar, como mínimo, con responsables, niveles de responsabilidad y sanciones en caso de incumplimiento. Enviar a la Contraloría General, a más tardar el 28 de febrero de 2018, una certificación que acredite la definición del procedimiento solicitado; y al 30 de abril de 2018 una certificación que acredite la implementación del respectivo procedimiento. Ver párrafos del 2.1 al 2.77 de este informe.

Firmamos a los 21 días del mes de diciembre de 2017, San José, Costa Rica.

Firmado digitalmente por JOSE LUIS ALVARADO VARGAS (FIRMA)

Lic. José Luis Alvarado Vargas
GERENTE DE ÁREA

CONTRALORIA GENERAL DE LA REPUBLICA * COSTA RICA *

Firmado digitalmente por MARIO ALBERTO PEREZ FONSECA (FIRMA)

M.Sc. Mario Alberto Pérez Fonseca
ASISTENTE TÉCNICO

MIGUEL PEREZ MONTERO (FIRMA)
Firmado digitalmente por MIGUEL PEREZ MONTERO (FIRMA)
Fecha: 2017.12.21 15:06:28 -06'00'

M.Sc. Miguel Pérez Montero
COORDINADORO