KPMG

Instituto Mixto de Ayuda Social (IMAS)

Carta a la Gerencia sobre la Valoración de las Normas Técnicas de la Contraloría para las Tecnologías de Información

19 de junio de 2018

KPMG, S.A.
Esta carta a la gerencia contiene 27 páginas.

KPMG S.A.
Edificio KPMG
San Rafael de Escazú
Costa Rica
+506 2201 4100

Señores
Consejo Directivo
Gerencia General
Tecnologías de la Información
Instituto Mixto de Ayuda Social
San José, Costa Rica
19 de junio de 2018

Estimados señores:

Hemos concluido nuestro auditoría de Tecnologías de Información del Instituto Mixto de Ayuda Social (en adelante "IMAS"), para reportar, al 31 de diciembre de 2017 y por el año terminado en esa fecha, sobre el cumplimiento de las Normas técnicas para la gestión y el control de las Tecnologías de Información, de conformidad con la Resolución de la Contraloría General de la República R-CO-26-2007, emitida el 7 de junio de 2007.

Producto de la evaluación se evidencia un cumplimiento parcial con las "Normas técnicas para la gestión y el control de las tecnologías de información (N-2-2007-CO-DFOE)". Se encontraron 12 hallazgos nuevos y se mantienen 7 hallazgos de auditorías de años anteriores.

Si bien se cuentan con procedimientos documentados para la mayoría de los procesos en el área de Tecnologías de Información, es necesario mejorar el cumplimiento efectivo de los mismos por parte del departamento y las áreas de negocio involucradas.

Es necesario considerar aspectos importantes con respecto a la Seguridad de la Información:

- Establecer personal encargado y formalizar un marco de Seguridad de la Información
- Concientización y compromiso de los empleados con la Seguridad de la Información
- Revisión y recertificación de usuarios en los sistemas (verificación de que los accesos de los usuarios son apropiados)
- Controles de acceso físico y de retiro de equipos
- Controles de borrado y desecho de discos duros

Adicionalmente es necesario reforzar en el manejo de contratos con proveedores tecnológicos tanto en la evaluación de los servicios provistos como el de actualización de contratos para establecer acuerdos de confidencialidad. El manejo del presupuesto de tecnología de información también debe tener un seguimiento regular y no solamente durante la formulación y aprobación del mismo. En lo que respecta al manejo de la Calidad en los servicios de TI se deben formalizar acuerdos de nivel de servicio con las áreas interesadas del negocio y medir el cumplimiento de los mismos. Adicionalmente se debe mejorar varios aspectos del plan de continuidad del negocio, incluido el desarrollo de un análisis de impacto del negocio y establecer los procesos críticos de TI.

KPMG S.A.
Edificio KPMG
San Rafael de Escazú
Costa Rica
+506 2201 4100

Finalmente es necesario documentar y formalizar un procedimiento para el manejo de cambios de software de manera que el proceso de desarrollo, pruebas, y liberación de cambios a producción tenga requerimientos claros.

Recalcamos que el resto de los procesos han resultado efectivos para los requerimientos de la normativa de la Contraloría. Adicionalmente se puedo evidenciar que se ha avanzado significativamente en la implementación de los planes de acción para los hallazgos de la auditoría del año pasado, quedando solamente unos 7 ítems pendientes.

Este informe fue discutido en forma de borrador con funcionarios de la Dirección de la jefatura de Tecnologías de Información del IMAS.

Si el Consejo Directivo, la Gerencia General, o la Jefatura de Tecnologías de Información tienen alguna observación con respecto al contenido de este informe, tendremos mucho gusto en ampliar cualquier aspecto a su solicitud.

Atentamente,

Erick Brenes F.
Socio

Timbre de ¢25 de Ley No. 6663
adherido y cancelado en el original

KPMG

Anexo I

Situaciones Identificadas al 31 de diciembre de 2017.

Como resultado de la revisión de las Normas técnicas para la gestión y el control de las tecnologías de información (N-2-2007-CO-DFOE)", se determinaron las siguientes situaciones:

Hallazgo 01: Incumplimiento de la Gestión de Calidad (1.2).	
Causa	▪ Con respecto al manejo de los incidentes, se determinó que no se le da seguimiento al cumplimiento del Procedimiento para la Administración de Incidentes (P-TI-02), que estipula que los tiquetes de la mesa de servicio deben ser cerrados posterior a su resolución.
Efecto	▪ No disponibilidad de información confiable y útil para la toma de decisiones con respecto a la mesa de servicios. ▪ Incumplimiento del desempeño de los servicios de TI en relación con lo estipulado; específicamente los tiempos de resolución de incidentes acordados
Recomendación	a. Asegurar por parte de las áreas involucradas el cumplimiento del procedimiento "P-TI-25 Procedimiento para la administración de incidentes", de manera que se cierren las solicitudes de mesa de servicios posterior a que son resueltas. b. Girar una circular recordando al personal apoyar al área de TI con respecto al "P-TI-25 Procedimiento para la administración de incidentes", de manera que los usuarios colaboren en dicho proceso y cierren los tiquetes a tiempo
Comentarios de la Administración	TI no tiene comentarios del hallazgo.

Hallazgo 02: Incumplimiento de la Gestión de Riesgos (1.3).	
Causa	▪ La revisión de la evaluación y la descripción de los controles identificados en la matriz de riesgos de TI no se lleva a cabo. Por lo tanto no hay una valoración objetiva y externa de control ▪ En el detalle de cada uno de los riesgos no se identifica la consecuencia asociada, lo que dificulta el análisis de la materialización del riesgo. ▪ No se cuenta con un cronograma de pruebas para garantizar la efectividad de los controles.
Efecto	▪ El incumplimiento de la gestión de riesgos a nivel de la identificación de controles puede resultar en un paro de operaciones de los servicios de TI e incluso de la institución debido a la ausencia de controles o a fallas en la efectividad de los controles relacionados a los riesgos.

Hallazgo 02: Incumplimiento de la Gestión de Riesgos (1.3).	
Recomendación	a. Definir la estrategia para apoyarse de conocimiento experto a la hora de valorar los controles asociados a los riesgos de TI. (Control Interno puede apoyarse en un especialista del área de TI en caso de no contar con personal especializado) Complementar el proceso de identificación de riesgos tomando en cuenta el factor de "consecuencia" con el fin de facilitar el análisis del impacto de la materialización de los riesgos. b. Ver recomendaciones de la Continuidad de los Servicios de TI (1.4.7) en referencia a las pruebas de efectividad de los controles.
Comentarios de la Administración	TI no tiene comentarios del hallazgo.

Hallazgo 03: Incumplimiento en la Implementación de un marco de seguridad de la información (1.4.1).	
Causa	▪ Se identificó que no hay una separación de las responsabilidades entre TI y Seguridad de la información. Las actividades del ámbito de seguridad de información garantizan la seguridad física y lógica de la información que se transmite en la infraestructura tecnológica. No hay un puesto de oficial o jefe de la Seguridad de la Información que asegure el cumplimiento de actividades tales como: o Asegurar la protección de todos los aspectos físicos y técnicos de la seguridad de la institución. o Elaboración de las políticas y procedimientos que aseguren el cumplimiento de las actividades diarias. o Recertificación periódica de usuarios en los sistemas. (verificación de que los accesos de los usuarios son apropiados) o Cumplimiento de las políticas relacionadas a la Administración de contraseñas. o Cumplimiento del proceso de solicitudes de acceso a los sistemas. ▪ La actividad de recertificación de usuarios para el uso de los sistemas tecnológicos no se lleva a cabo periódicamente, por lo tanto no hay un control acerca del acceso a la información por parte de los colaboradores de acuerdo a las responsabilidades de su puesto.
Efecto	▪ Debilidades en el cumplimiento de las actividades que resguarden la seguridad de la información de la Institución.
Recomendación	a. Analizar la posibilidad de abrir una plaza de Oficial de Seguridad de Información con su perfil de puesto, roles y responsabilidades establecidas y aprobadas formalmente. Entre las responsabilidades a asumir por el Oficial de Seguridad de la Información se encuentran: 1. Establecer un representante de la institución que atienda las consultas de los usuarios, gerencia y público en general acerca de la estrategia de seguridad de la información. 2. Establecer un representante que apoye los trámites legales de la institución en situaciones de investigación de funcionarios.

Hallazgo 03: Incumplimiento en la Implementación de un marco de seguridad de la información (1.4.1).	
	3. Asegurar la divulgación y concientización del personal acerca de la importancia de la seguridad de la información con un plan de capacitación oportuno y que reciba seguimiento de cumplimiento por el Comité Gerencial de TI. 4. Supervisar, evaluar y valorar un sistema que garantice el control de salida e ingreso tanto del personal como de los equipos tecnológicos. 5. Establecer un sistema de control de acceso a los sistemas de TI de la institución por medio de actividades de recertificación de usuarios periódicas con el fin de asegurar el uso correcto de los sistemas por medio de las recertificaciones. b. En el periodo interino mientras se resuelve la posibilidad de una plaza de una persona que se encargue de la seguridad de la información, TI debería al menos realizar una recertificación de usuarios para los sistemas críticos (por ejemplo: SAP y algunos de los sistemas sociales)
Comentarios de la Administración	TI procederá a remitir los listados de usuarios y perfiles activos a las jefaturas de las áreas para que verifiquen si las personas funcionarias pertenecen a sus áreas y con dichos perfiles para depurar cualquier cambio que sea reportado por las mismas.

Hallazgo 04: Incumplimiento de las actividades de seguridad física y ambiental (1.4.3).	
Causa	▪ Con respecto a la seguridad perimetral, se determinó que en la entrada principal del IMAS no se lleva un control estricto de la entrada y salida de personal. Se determinó que en repetidas ocasiones la revisión y el registro del personal no se llevó a cabo. ▪ Adicionalmente, el ingreso y salida de los equipos de la organización debe estar autorizada por el Jefe del área de TI. Sin embargo no se lleva un control que identifique la entrada o salida del equipo con el objetivo de verificar que se cumplan los lineamientos establecidos. ▪ No se lleva a cabo un control completo acerca del ciclo de vida de los activos. Por lo tanto no se establece un procedimiento formal para el desecho y la reutilización de los activos. Si bien se realiza formateo de los discos duros previo a desecharlos no se cuenta con un inventario de los discos duros que se van desechando para tener un control de cuales discos han sido formateados ▪ De igual manera no se lleva un control detallado acerca de las actividades realizadas en el equipo tecnológico a la hora del mantenimiento. ▪ Se encontraron cables telefónicos mal acomodados en los cuartos de comunicación, especialmente en el primer piso
Efecto	▪ Mal uso o la manipulación mal intencionada de la información tanto pública como sensible almacenada en los sistemas de TI del I.M.A.S. ▪ Revelación al público de datos sensibles almacenados en equipos de desecho.

Hallazgo 04: Incumplimiento de las actividades de seguridad física y ambiental (1.4.3).	
Recomendación	a. Reforzar los controles de entrada a las instalaciones, así como los controles de ingreso y salida de equipos. b. Corregir la colocación de los cables telefónicos en los cuartos de comunicación (especialmente el del primer piso) c. Confeccionar un documento (o ampliar el procedimiento de activos existente) identificando las diferentes etapas del ciclo de vida, específicamente para los activos tecnológicos con el propósito de darle seguimiento y asegurar el cumplimiento de cada una de las etapas, tomando como referencia métricas o estándares de calidad y cumplimiento. El documento debe tomar en cuenta: a. El paso de adquisición del equipo b. El paso de asignación y re-asignación de equipos a cada área c. Reforzar y documentar los controles para la etapa de desecho del equipo, especialmente el manejo de un inventario del equipo a ser desechado. (en coordinación con la Jefatura de TI para el borrado de la información)
Comentarios de la Administración	Sobre la seguridad perimetral se indica: a) Existe una cláusula en el contrato de vigilancia que establece que los oficiales de turno deben revisar a cualquier persona que ingresa a la institución y que porte equipo personal o maletines. Además, existe un procedimiento instruido a la empresa de seguridad y sus oficiales, el cual consiste en que, el oficial toma nota de los datos del equipo que ingresa o sale, y lo registra en la bitácora, en el caso de los equipos que tienen el formulario autorizado de ingreso o salida creado para ese efecto, se archiva en el expediente y permanece en custodia de los oficiales. Sobre los cables del cuarto de comunicación: a) Se procederá a realizar el ordenamiento de los cables telefónicos del primer piso. Sobre el procedimiento de activos, se cuenta con el Manual de Procedimiento de Control de Activos Institucionales MP-API-03, que cubre lo solicitado por esta recomendación. De hecho, está seccionado e incluye las partes de compra, asignación, reasignación y desecho (con las opciones para el mismo). El Área de TI actualizará la "*Boleta de Servicios Prestados de TI*" para que se incluya un "check" para que el soportista lo marque cuando la actividad fue revisión para desecho y que se garantiza con esto que la información en el disco duro fue eliminada en su totalidad.

Hallazgo 05: Incumplimiento de controles de seguridad en las operaciones (1.4.4).	
Causa	▪ Se cuenta con el sistema de antivirus Symantec Endpoint Protection sin embargo mediante de observación de uno de los reportes semanales se determinó que no se le está dando un seguimiento a los reportes con el fin de identificar posibles controles preventivos, detectivos y correctivos basados en la información recolectada. ▪ Se determinó que no se cuenta con un control o procedimiento para la actualización de las contraseñas de los diferentes puntos de accesos de internet inalámbrico (WIFI) de la Institución y que la última vez que las contraseñas fueron modificadas fue hace más de un año atrás.
Efecto	▪ Mal uso o la manipulación mal intencionada de la información tanto pública como sensible almacenada en los sistemas de TI del I.M.A.S. por programas maliciosos. ▪ Si bien las redes WIFI están separadas de las redes institucionales, todavía es posible que terceros malintencionados con acceso a las contraseñas roben información de laptops o dispositivos institucionales que se encuentren conectados a las redes WIFI
Recomendación	a. Llevar a cabo un análisis periódico de las actividades frecuentes en el reporte del antivirus con la finalidad de formar una base de conocimiento e identificar nuevos riesgos y controles para TI. b. Establecer un proceso o directriz que dicte los lineamientos para una Administración de contraseñas de los accesos inalámbricos, de manera que estas se cambien periódicamente.
Comentarios de la Administración	TI en el año 2018 designó a los técnicos en soporte del área para dar el seguimiento a la consola de antivirus. Se girará las instrucciones para realizar las revisiones de los reportes de antivirus para generar base de conocimiento y tomar medidas preventivas y correctivas oportunamente. En cuanto al tema de la red wi-fi: TI ya tiene el acceso wi-fi separado de la red principal por lo que se girarán instrucciones al personal interno de TI encargado del wi-fi para generar la tarea de cambio de contraseñas al wi-fi según la política institucional para cambios de contraseñas.

Hallazgo 06: Incumplimiento en las actividades de seguridad en la implementación y mantenimiento de software e infraestructura tecnológica (1.4.6).	
Causa	▪ No se lleva un control periódico del acceso a los programas fuente y datos de prueba. ▪ En relación con los ambientes de trabajo, en el caso del sistema de Desarrollo Humano, no se cuenta con una separación de ambientes para el código fuente.
Efecto	▪ Incumplimiento de los requerimientos alineados a las necesidades de negocio al implementar software o infraestructura. ▪ Posibles errores en la pases a producción de los cambios en los sistemas debido a falta de claridad con respecto al proceso de cambios

Hallazgo 06: Incumplimiento en las actividades de seguridad en la implementación y mantenimiento de software e infraestructura tecnológica (1.4.6).	
Recomendación	a. Establecer un sistema de control de acceso al código fuente y datos de prueba de los sistemas de TI (Sistemas Sociales, Desarrollo Humano y Sistemas Comerciales), de la institución por medio de actividades de recertificación de usuarios periódicas.
Comentarios de la Administración	TI no tiene comentarios del hallazgo.

Hallazgo 07: Mejoras requeridas al control de la continuidad de los servicios de TI (1.4.7).	
Causa	▪ Se determinó que el plan de continuidad no está completamente alineado con la matriz de riesgos de TI que es manejada por la unidad de TI. Se deben alinear los riesgos de continuidad de TI con el plan. ▪ Se determinó que el diseño y efectividad del Plan de Continuidad requiere algunas mejoras. El Plan de Continuidad para ser oficial debe contener una sección de pruebas que evidencie la efectividad del Plan. Debido a que se hace la selección de un solo control para riesgos críticos por año para valorar la efectividad, es necesario llevar una bitácora con las actividades o pruebas elegidas en el año en curso, con la finalidad de que en algún momento se tenga documentada con al menos una prueba para cada uno de los controles.
Efecto	▪ Paro parcial o total de las operaciones del IMAS por riesgos de continuidad no cubiertos por el plan.
Recomendación	a. Establecer un espacio entre el área de TI y el área de riesgos en el cual se pueda: 1. Identificar la criticidad de cada uno de los procesos de TI. 2. Identificar los riesgos de continuidad asociados a los procesos críticos de TI. 3. Establecer los controles necesarios para mitigar estos riesgos (Con la colaboración de un usuario especializado que tenga responsabilidad en el cumplimiento de estos controles) 4. Identificar los escenarios de activación del plan de continuidad. 5. Establecer el orden de revisión de los controles de los riesgos basado en el nivel de criticidad y llevar una bitácora con las revisiones por cada año.
Comentarios de la Administración	TI no tiene comentarios del hallazgo.

Hallazgo 08: Incumplimiento de la gestión de proyectos (1.5).	
Causa	▪ A partir de las reuniones de entendimiento, se determinó que a nivel general no se cuenta con una Oficina de Administración de Proyectos (PMO, por sus siglas en ingles) que centralice la Administración y el seguimiento a los proyectos. Adicionalmente, referente al departamento de TI, no se ha formalizado la diferencia a nivel de proceso entre lo que conlleva administrar un proyecto y la atención de solicitudes de requerimientos o de mantenimiento en los sistemas.
Efecto	▪ Falta de compromiso de las áreas interesadas en los programas y proyectos al no tener un responsable que vele por el cumplimiento de los procedimientos. ▪ Incumplimiento del logro de los beneficios esperados de los programas y proyectos.
Recomendación	a. Determinar un responsable del cumplimiento y seguimiento para los proyectos del área de TI (o bien una PMO institucional, el que resulte más conveniente de acuerdo a la valoración de la Gerencia) para poder cuantificar su valor y calidad en relación con el cumplimiento de los objetivos estratégicos de TI. b. Separar la metodología de proyectos del proceso que documenta el manejo de cambios en TI
Comentarios de la Administración	El PEI tiene un componente de revisión de estructura, estudio cargas de trabajo; donde se aprovechará para estudiar la viabilidad de una oficina de Proyectos.

Hallazgo 09: Incumplimiento de las obligaciones relacionadas con la gestión de TI (1.7).	
Causa	▪ En la Política para Clasificación y uso de la Información POL-01 se hace referencia a artículos de las leyes referentes a la gestión de TI con la finalidad de tener claro y velar por el cumplimiento del marco jurídico aplicable. Sin embargo no se identifica el mecanismo para garantizar el cumplimiento de estas leyes. Una de las leyes que se menciona es la N°8454, Ley de certificados, firmas digitales y documentos electrónicos quedando por fuera leyes como Delitos Informáticos (Ley N 8148), Protección de la Persona Frente al Tratamiento de sus Datos personales (Ley N° 8968).
Efecto	▪ Materialización de posibles conflictos legales ocasionados por el incumplimiento del marco jurídico y leyes aplicables.
Recomendación	a. Incluir la aplicación de las leyes relacionadas a TI dentro de las actividades de clasificación de la información así como en los procesos de TI que lo amerite. Asimismo debe incluir el mecanismo para garantizar el seguimiento y cumplimiento de estas leyes. b. Verificar el cumplimiento de la institución en los temas de Normativa aplicable a Tecnologías de Información

Hallazgo 09: Incumplimiento de las obligaciones relacionadas con la gestión de TI (1.7).	
	c. Ver recomendaciones del punto: Implementación de un marco de seguridad de la información (**1.4.1**) relacionado al cumplimiento del marco jurídico que influya en la gestión de TI (**a-2**). d. Considerar la posibilidad de asignar una unidad de cumplimiento institucional que vele por la mitigación de cumplimiento legal a nivel general
Comentarios de la Administración	No hay comentarios.

Hallazgo 10: Fallas de control del cumplimiento de los acuerdos de servicios (4.1).	
Causa	▪ Se evidenció que se cuenta un Procedimiento para la Definición de Acuerdos de Niveles de Servicio (P-TI-18), así como el Acuerdo de Nivel Operativo (OLA) que no tiene un código de referencia para identificarlo. Dentro del OLA se lista el catálogo de servicios sin embargo no se detallan las métricas de evaluación de los acuerdos y por lo tanto se dificultan las actividades de seguimiento y de cumplimiento.
Efecto	▪ Desconocimiento de los servicios tanto de TI como de la institución para un uso efectivo de los recursos ▪ Falta de claridad sobre los tiempos de respuesta y las expectativas sobre cuando se resolverán los incidentes tecnológicos
Recomendación	a. Actualizar el OLA para que integre las métricas de servicios de telecomunicaciones ya establecidas b. Considerar la definición de métricas de disponibilidad de los sistemas críticos dentro del OLA (ejemplo: disponibilidad del 70%), negociar dichas métricas en conjunto con la Gerencia General y con los interesados del negocio c. Establecer un nivel de servicio (tiempo de respuesta) para la atención de solicitudes de la mesa de servicio, dicho acuerdo puede incluirse en el OLA o bien en un documento aparte del SLA. Dichos tiempos de respuesta deberán variar de acuerdo a la criticidad de la solicitud. Estos acuerdos deberán ser establecidos en conjunto con la Gerencia General y las áreas interesadas del negocio d. Para todos los puntos anteriores la Jefatura de TI deberá contar con una provisión de recursos (personal, financieros, y de infraestructura) que le permita cumplir con dichos niveles y horarios de servicio
Comentarios de la Administración	TI no tiene comentarios del hallazgo.

Hallazgo 11: Incumplimiento de las revisiones periódicas de los servicios prestados por terceros (4.6).	
Causa	▪ Se determinó que no se establecen mediciones de efectividad de los servicios brindados por los proveedores; de manera que satisfagan las necesidades del negocio.
Efecto	▪ Incumplimiento de los servicios acordados por los proveedores
Recomendación	a. Considerar la contratación de una persona dentro del área de TI encargada de los temas de compras y la Administración de las relaciones con los proveedores de tecnología. b. Realizar evaluaciones regulares sobre la calidad de los servicios brindados por los proveedores de TI de manera que se puedan tomar decisiones cuando los servicios recibidos no sean adecuados las necesidades de la institución. c. Instruir a que los administradores de contrato realicen evaluaciones regulares sobre la calidad de los servicios brindados por los proveedores tecnológicos (que no sean coordinados por el área de TI) de manera que se puedan tomar decisiones cuando los servicios recibidos no sean adecuados las necesidades de la institución.
Comentarios de la Administración	De acuerdo con el Área de Proveeduría Institucional, existe una evaluación de la efectividad de las entregas, calidad del producto, atención y servicio al cliente, esto una vez concluida la contratación. La misma se realiza en el sistema de compras designado (en este momento SICOP). Para la evaluación parcial o durante el contrato, le corresponde al administrador del contrato comunicar activamente a la Gerencia General de las anomalías y cualquier falla en la calidad o servicio contratado, el mismo está claramente definido en la Directriz GG-2076-10-2017 con respecto a la fiscalización de contratos.

Hallazgo 12: Brechas en el seguimiento y evaluación del control interno de TI (5.2).	
Causa	▪ Se determinó que no hay un trabajo en conjunto por parte de TI y Control Interno que asegure la evaluación de la efectividad y el cumplimiento, así como mantener una bitácora de las excepciones presentadas y de las medidas correctivas que se le aplicaron.
Efecto	▪ Incumplimiento de TI con las políticas internas ▪ Brechas en el cumplimiento de la Administración del riesgo por TI
Recomendación	a. Establecer un plan de trabajo entre TI y Control Interno que permita la identificación de los controles críticos y la evaluación de la efectividad y el cumplimiento de las actividades de la Gestión de TI.
Comentarios de la Administración	No hay comentarios.

KPMG

Situaciones de la auditoría de años anteriores que siguen pendientes.

Se detallan situaciones con respecto a hallazgos de auditorías de años anteriores que siguen pendientes, así como recomendaciones actualizadas para las mismas.

Seguimiento 01: Incumplimiento del plan de capacitación del personal para el 2017 (Cumplimiento de la auditoría anterior –hallazgo 13-).	
Causa	▪ No se llevó a cabo un plan de capacitación para el personal de TI en el año 2017.
Efecto	▪ El desconocimiento del personal acerca de la seguridad de la información puede resultar en un uso inadecuado o mal intencionado por parte del personal comprometiendo la integridad de la institución.
Recomendación	a. Incluir en la estructura del plan de inducción una sección que haga referencia a las buenas prácticas del uso de la información de la institución. b. Establecer un plan de capacitación para el personal de TI que incluya temas alineados con el cumplimiento de los objetivos estratégicos del PETI. c. Asegurar el cumplimiento y desarrollo de estos planes así como un método de evaluación para valorar los conocimientos adquiridos en los planes.
Comentarios de la Administración	Punto a) La recomendación ya está incluida en la inducción. Se hace en la inducción la parte de información y la confidencialidad, además se incluye un CD que se entrega a la persona de ingreso la normativa que aplica en la institución, del manejo de información, así como del folleto del código de ética y valores institucionales. Punto b) Ya se hace un plan y en este se incluyen las solicitudes remitidas por TI. Punto c) DH efectúa una evaluación de las capacitaciones a los 3 meses de recibida por la persona funcionaria. TI remitió oficio TI-119-05-2017 a Desarrollo Humano, con la solicitud de necesidades de capacitación para 2018. Adicionalmente a esta acción, que se realiza operativamente todos los años, se solicitó y ejecutó reunión con DH el 12 de octubre 2017 para analizar el tema específico de TI. Se continuará remitiendo en forma anual antes del cierre de plan presupuestario de cada año, las necesidades de capacitación para el año siguiente. Corresponderá a DH comunicar en forma anual el Plan de Capacitación. Además, según se hace constar en los oficios DH-3788-12-2017, Desarrollo Humano notifica que con el oficio TI-270-11-2017 se da por cumplido el proceso correspondiente a 2017. Queda pendiente para noviembre 2018 realizar el proceso de revisión correspondiente a este año.

Seguimiento 02: Incumplimiento del Marco Estratégico de TI. (Cumplimiento de la auditoría anterior – hallazgo 06-).	
Causa	▪ Se identifican debilidades en el Plan Estratégico de TI (PETI), de las cuales; El plan de acción no está alineado con la cantidad de objetivos estratégicos por lo que no se está planificando la totalidad del programa. Se identificaron cinco objetivos estratégicos y el plan estratégico solo tomaba en cuenta tres de ellos. ▪ A partir de los informes trimestrales se identificó que este incluye la información acerca del Plan Operacional Gerencial (POGE) y no de del seguimiento adecuando al cumplimiento de los objetivos del PETI. ▪ A partir de la falta de madurez identificada en el Plan Estratégico de TI (PETI) en relación al proceso de seguimiento y cumplimiento del mismo, se identifica una dificultad para darle seguimiento a las decisiones del Jerarca sobre asuntos estratégicos.
Efecto	▪ Disrupción del alineamiento entre la estrategia de negocio y de TI. ▪ Dificultades para el Comité Gerencial de TI para tomar decisiones. ▪ Ausencia de estructura organizativa para la optimización de los activos, recursos y capacidades de TI. ▪ Incumplimiento de la visión y las metas del jerarca por falta de organización.
Recomendación	a. Llevar a cabo una revisión del alineamiento de los objetivos estratégicos con el plan de acción para asegurar su cumplimiento. b. Garantizar la revisión formal y periódica de los indicadores de calidad y satisfacción para cada una de las actividades del plan de acción. c. Asegurar que se le dé seguimiento al cumplimiento de los objetivos establecidos en el PETI dentro de las reuniones trimestrales de seguimiento del Comité Gerencial de TI.
Comentarios de la Administración	Se completó el proceso de alineamiento del PETI con el PEI en Junio 2018. La actualización del PETI se encuentra, en la etapa de revisión y aprobación por parte del Consejo Directivo.

Seguimiento 03: Incumplimiento de la Gestión de Calidad (Cumplimiento de la auditoría anterior – hallazgo 11-).	
Causa	▪ Se evidenció una brecha en la eficiencia en el control de la calidad debido al no cumplimiento de las evaluaciones del sistema de gestión de la calidad. Actualmente en múltiples ocasiones el personal de TI ha tenido que dar las solicitudes de la mesa de servicios por cerradas debido a que el solicitante no le da seguimiento a la solicitud. La situación anterior altera los tiempos de cumplimiento de las solicitudes, lo cual afecta los reportes de capacidad de la mesa servicios.
Efecto	▪ No disponibilidad de información confiable y útil para la toma de decisiones con respecto a la mesa de servicios. ▪ Incumplimiento del desempeño de los servicios de TI en relación con lo estipulado; específicamente los tiempos de resolución de incidentes acordados
Recomendación	Divulgar la importancia del cumplimiento y las responsabilidades del proceso de Administración de incidentes acorde a lo establecido en el documento "P-TI-25 Procedimiento para la Administración de incidentes".
Comentarios de la Administración	TI separó la divulgación solicitada en tres distintas fechas: mayo y octubre 2018 y febrero 2019. La correspondiente a mayo se realizó el miércoles 16 de mayo de 2018 a las 08:13 am vía correo-e a todo el funcionariado institucional.

Seguimiento 04: Incumplimiento del compromiso del personal con la seguridad de la información (Cumplimiento de la auditoría anterior –hallazgo 13-).	
Causa	▪ Debido a la falta del Marco de Seguridad de la Información y de un Oficial de Seguridad de la información, no se evidenció un compromiso con la seguridad de la información a nivel Institucional. Actualmente, esta actividad se lleva a cabo por parte del área de Desarrollo Humano (DH) en conjunto con el área de TI. Las áreas interesadas deben informar al área de DH cuáles son las necesidades a con el fin de confeccionar el plan de capacitación. Sin embargo, se determinó que para el año 2017 no se impartió ninguna capacitación en relación con la seguridad de la información.
Efecto	▪ La ineficiencia en la Administración de los recursos humanos en temas de compromiso y buen uso de las prácticas de seguridad de la información puede dar paso a un uso inadecuado de la información del público almacenada en los sistemas así como de la información sensible de la institución.
Recomendación	a. Formalizar un plan de capacitación anual para asegurar el compromiso de los empleados en temas de seguridad de la información
Comentarios de la Administración	TI no tiene comentarios para seguimiento.

Seguimiento 05: Ausencia de revisión del cumplimiento de la política de la clasificación de la información (Cumplimiento de la auditoría anterior –hallazgo 3, periodo 2014-).	
Causa	▪ No se identificó un método que verifique el cumplimiento de la clasificación de la información, incluyendo una identificación de la sensibilidad de la información almacenada en los sistemas.
Efecto	▪ Paro de operaciones o fallos en los sistemas por falta de controles oportunos para el accesos a los sistemas de TI del IMAS. ▪ Acceso indebido a información institucional por parte de colaboradores que retienen accesos de puestos anteriores.
Recomendación	a. Los recursos de TI deben clasificarse formalmente, con el propósito de asegurar un nivel de protección óptimo dependiendo de la sensibilidad y criticidad de la información que esta guardada en ellos. Esta clasificación debe pasar por un proceso de revisión periódico. De manera que se asegure que los equipos con información de nivel sensible y confidencial estén debidamente protegidos.
Comentarios de la Administración	TI no tiene comentarios para seguimiento.

Seguimiento 06: Incumplimiento en las actividades de seguridad en la implementación y mantenimiento de software e infraestructura tecnológica (Cumplimiento de la auditoría anterior – hallazgo 09-).	
Causa	▪ No se identifica un procedimiento referente a la puesta en producción de software e infraestructura. Además de que se cuenta con una variedad de sistemas por lo que algunas de las etapas del proceso podrían variar.
Efecto	▪ Incumplimiento de los requerimientos alineados a las necesidades de negocio al implementar software o infraestructura. ▪ Posibles errores en la pases a producción de los cambios en los sistemas debido a falta de claridad con respecto al proceso de cambios
Recomendación	a. Elaborar el documento que establezca los lineamientos para las actividades de puesta en producción tanto en software como en infraestructura. Así como establecer los controles para garantizar el cumplimiento de estas actividades.
Comentarios de la Administración	El procedimiento de la metodología del estándar de desarrollo está pronto a concluirse para someterlo a aprobación.

Seguimiento 07: Brechas en las consideraciones de la implementación de TI (Cumplimiento de la auditoría anterior –hallazgo 09-).	
Causa	▪ A partir de reuniones con el área de TI, se determinó que no se cuenta con un documento que establezca los lineamientos a seguir a la hora de implementar cambios en los sistemas de TI. La Metodología de Proyectos es solamente aplicable ante un proyecto y no para cambios. El proceso de solicitud y atención de cambios debe ser independiente del proceso de gestión de proyectos. ▪ No se cuenta con el procedimiento de Implementación de Software lo que dificulta el control de las actividades que se llevan a cabo así como la calidad y el cumplimiento para garantizar el lineamiento con los objetivos estratégicos del PETI.
Efecto	▪ Ausencia de un proceso de aprobación para las solicitudes de cambio, que puede resultar en cambios indebidos y no autorizados que afecten la funcionalidad y la disponibilidad de los sistemas de información del IMAS.
Recomendación	a. Elaborar el procedimiento formal que describa el proceso de metodología de cambios, además de determinar que se va a usar parar valorar la calidad de los cambios y garantizar el cumplimiento de estos en relación con las métricas de calidad. Valorar si se debe modificar algún procedimiento relacionado con la metodología de cambios o bien crear uno por aparte.
Comentarios de la Administración	TI cuenta con la "Política para la implementación de soluciones de TI" (POL-EDI-20) y el "Procedimiento para la implementación de soluciones de TI" (P-TI-15) los cuales contemplan lo solicitado por la auditoría en esta recomendación. Sin embargo, consideramos importante mencionar que vemos oportuno realizar la revisión y actualización de los mismos; por lo que están contemplados para ser revisados como parte del Diagnóstico de normativa de TI que actualmente cuenta con autorización de Gerencia General GG-1241-06-2018 para realizarlo de acá hasta diciembre 2020 para alinearlos con los planes estratégicos de TI.

KPMG

Matriz de Riesgos Institucional de las situaciones identificadas al 31 de diciembre de 2017.

A continuación presentamos un detalle de la matriz de riesgos institucionales identificados en el periodo sujeto a revisión:

Capítulo de referencia	Riesgo Inherente	Probabilidad	Impacto
1. Normas de aplicación general	Disrupción del lineamiento entre la estrategia del negocio y de TI causado por bajo nivel de madurez del Plan Estratégico de TI (PETI) referente al plan de acción para el cumplimiento de los objetivos estratégicos del negocio	3. Posible	3. Moderado
	Carencia de decisiones estratégicas por parte del Comité Gerencial de TI a causa de la falta de seguimiento adecuado al PETI.	3. Posible	4. Alto
	No disponibilidad de información confiable y útil para la toma de decisiones causada por la falta de cumplimiento de las evaluaciones de sistema de gestión de calidad.	3. Posible	2. Menor
	Incumplimiento del desempeño oportuno de los servicios de TI a causa de la ausencia de seguimiento al cumplimiento del procedimiento para la Administración de incidentes.	3. Posible	3. Moderado
	Incumplimiento de la gestión de riesgos a nivel de la identificación de los controles puede resultar en un paro de operaciones de los servicios de TI y de la Institución debido a la ausencia de controles o a fallas en la efectividad de los controles.	4. Muy probable	3. Moderado
	Brechas de seguridad en las actividades que resguardan la seguridad de la información de la Institución debido a la ausencia de un responsable del cumplimiento de la Seguridad de la Información.	4. Muy probable	3. Moderado
	Uso inadecuado de la información sensible de la institución a causa de la ausencia de un marco de la seguridad de la información.	4. Muy probable	3. Moderado
	Uso inadecuado o pérdida de información o activos como consecuencia de los controles perimetrales de la institución.	3. Posible	3. Moderado
	Mal uso o la manipulación mal intencionada de la información tanto pública como sensible almacenada en los sistemas de TI del I.M.A.S. causado por el bajo control de programas maliciosos en los sistemas del I.M.A.S.	3. Posible	3. Moderado

Capítulo de referencia	Riesgo Inherente	Probabilidad	Impacto
	Incumplimiento de los requerimientos alineados a las necesidades de negocio al implementar software o infraestructura causado por ausencia de formalización de procesos para la implementación y mantenimiento de software e infraestructura.	3. Posible	3. Moderado
	Paro parcial o total de las operaciones del IMAS causado por el desconocimiento de la calidad de las pruebas de efectividad de los controles de continuidad.	3. Posible	4. Alto
	Mala asignación y uso de los recursos causado por la ausencia de un responsable que ejecute de manera oportuna los programas y proyectos.	3. Posible	3. Moderado
	Materialización de conflictos legales ocasionados por el incumplimiento del marco jurídico y leyes aplicables.	3. Posible	3. Moderado
	Dificultades de entendimiento, monitoreo y cumplimiento de la arquitectura e infraestructura de la plataforma tecnológica a causadas por la informalidad de los diagramas que la representan.	4. Muy probable	4. Alto
2. Planificación y organización	Inadecuado uso de los recursos financieros asignados a la gestión de TI en consecuencia de la falta de seguimiento y cumplimiento al plan de compras anual de TI.	3. Posible	3. Moderado
	Incumplimiento de los objetivos estratégicos del negocio causado por la falta de un procedimiento de implementación de software que asegure el cumplimiento y la calidad.	3. Posible	3. Moderado
3. Implementación de tecnologías de información	Cambios indebidos o no autorizados en la implementación de software causados por la falta de un procedimiento de implementación de software que asegure el cumplimiento y la calidad.	3. Posible	3. Moderado
	Incumplimiento del desempeño acorde a lo objetivos estratégicos de TI por parte de los terceros contratados como consecuencia de la falta de una plantilla estándar que incluya las cláusulas que competan.	3. Posible	3. Moderado
	Mala gestión de los recursos de TI a causa del desconocimiento de los productos y servicios del departamento.	3. Posible	2. Menor
4. Prestación de servicios y mantenimiento	Incumplimiento de los objetivos estratégicos de TI a causa de la falta de claridad acerca de los tiempos de respuesta y las expectativas sobre tiempos de resolución	3. Posible	2. Menor

Capítulo de referencia	Riesgo Inherente	Probabilidad	Impacto
	Incumplimiento de las actividades operativas alineadas a los objetivos estratégicos de la Institución como consecuencia de la falta de un mecanismo de vigilancia que permita monitorizar la disponibilidad, capacidad, desempeño y uso de la plataforma tecnológica.	3. Posible	3. Moderado
	Paro de operaciones total o parcial causado por la falta de control de la separación de ambientes para el código fuente de los sistemas	3. Posible	2. Menor
	Incumplimiento de los servicios acordados por los proveedores a causa de la ausencia de mediciones periódicas de la efectividad de estos servicios.	3. Posible	3. Moderado
	Incumplimiento de las políticas internas causado por la falta de un sistema de valoración de las metas y métricas de los procesos de TI.	3. Posible	4. Alto
5. Seguimiento	Incumplimiento de las políticas internas a causa del bajo nivel de comunicación entre el área de TI y Control Interno.	3. Posible	4. Alto

Anexo II

Seguimiento a Situaciones de Periodos Anteriores.

Hallazgo 01: No se revisan las pistas de auditoría de los sistemas de información del IMAS. (1.4.5)	
Riesgo	Medio
Recomendación	En primera instancia con el fin de reducir el impacto y las ocurrencias de los incidentes de seguridad dentro del nivel del apetito de riesgo de la institución es indispensable definir, operar y monitorizar un sistema para la Administración de la seguridad. • Valorar la necesidad de la revisión de pistas de auditoría de control de acceso a los sistemas de información del I.M.A.S. basado en la criticidad de estos. • La actividad de revisión de las pistas de auditoría de los accesos de los sistemas de información del I.M.A.S. podría remplazarse por recertificaciones periódicas de los sistemas de información de la institución (Ver recomendaciones del hallazgo 8 del auditoría anterior). • Esta actividad debería considerarse como parte de los controles asociados a los riesgos de la Seguridad de la Información (SI). Y por ende contar con los mecanismos aseguren el monitoreo y el cumplimiento de estos controles. • El área de Control Interno es quien debe cooperar para asegurar el cumplimiento de estos controles.
Acciones de Remediación	**Seguimiento.** Debido a que los sistemas están administrados por diferentes áreas, en el documento "PR-TI-07 Procedimiento para la Administración de accesos, cuentas de personas usuarias y perfiles o roles", se delega la responsabilidad de la revisión de las bitácoras a cada uno de los Jefes de área que administran estos sistemas.
Estado	Actualmente se procedió a actualizar el documento "PR-TI-07 Procedimiento Administración accesos cuentas usuarias perfiles roles", el cual fue aprobado por la gerencia y divulgado a lo largo de la institución. La fecha de divulgación data de diciembre del 2017 por lo que no fue posible contar con documentación que evidenciara el cumplimiento de lo establecido. Adicionalmente no se establece un dispositivo para monitorear el control y cumplimiento periódico de esta tarea.

Hallazgo 02: Inexistencia de un plan de pruebas para el plan de continuidad de TI. (1.4.7)	
Riesgo	Medio
Recomendación	**No se identifican recomendaciones para este hallazgo.** La importancia de la efectividad de un plan de continuidad es asegurar la continuidad de las operaciones críticas de negocio y mantener la disponibilidad de la información a un nivel aceptable. Es indispensable establecer, operar y monitorear un plan que permita al departamento de TI responder ante cualquier tipo de incidentes o disrupciones con el fin de continuar con las operaciones críticas del negocio. Además
Acciones de Remediación	**Cumplido.** Ya se aprobó el documento "Plan Anual de Pruebas de Restauración ante Contingencias de TI" por parte de la Gerencia General para ponerse en práctica a partir de Enero del 2018. El cual cumple con las recomendaciones establecidas por la auditoría anterior.
Estado	Actualmente, ya el documento "Plan Anual de Pruebas y Restauración ante Contingencias de TI" ha sido aprobado por parte de la Gerencia General. Este plan cumple con las recomendaciones de estructura establecidas por la auditoría anterior con respecto a los detalles del proceso así como el análisis de los resultados. Este plan fue remitido en Diciembre del 2017 por lo tanto no fue posible evaluar la efectividad por el alcance de la auditoría en curso.

Hallazgo 03: Cumplimiento parcial del reglamento gerencial de tecnologías de información. (1.6)	
Riesgo	Bajo
Recomendación	Con el fin de garantizar el cumplimiento y el objetivo de las reuniones del Comité Gerencial de Tecnologías de Información, se sugiere lo siguiente: • Las minutas de actividad y acuerdos de estas sesiones deben ser remitidas periódicamente a la Junta Administrativa con el fin de darle seguimiento al cumplimiento de las metas de TI así como asegurar el lineamiento de estas metas con las de negocio de la institución.
Acciones de Remediación	**Parcialmente cumplido.** A partir de las reuniones se determinó que no se le da el seguimiento adecuado al PETI durante estas sesiones. Más bien, se valora el cumplimiento del Plan Organizacional Gerencial (PETI).
Estado	La documentación analizada del periodo 2017, cuenta con siete minutas de asistencia y cinco documentos de minutas de actividad. Con respecto a la asistencia, dentro de estos siete documentos de los 12 esperados, se identificó que en todos hacen falta al menos una o más firmas de los miembros participantes. Con respecto a las minutas de actividad, no todas hacen mención a temas relacionados con las metas o el cumplimiento del área de TI. Dos de las cinco mencionan acuerdos al final de la reunión ligados a las tecnologías de

Hallazgo 03: Cumplimiento parcial del reglamento gerencial de tecnologías de información. (1.6)	
	información. Sin embargo para las minutas que si se dirigen a las metas o el cumplimiento de las actividades de TI, no se establece un mecanismo de seguimiento y control para garantizar finalización estos acuerdos. Este mecanismo debería identificar a los responsables de los procesos, los responsables del cumplimiento, las actividades a efectuar y las fechas límites.

Hallazgo 04: Debilidades en la seguridad física del cuarto de servidores y cuartos de comunicaciones del IMAS. (1.4.3)	
Riesgo	Medio
Recomendación	**No se identifican recomendaciones para este hallazgo.** La relevancia de un control estricto de seguridad física radica en velar por la integridad de los activos físico, comúnmente críticos, con el propósito cumplir con los estándares de calidad en la entrega de los productos y servicios de TI.
Acciones de Remediación	**Cumplido.** Para satisfacer la recomendación de la auditoría anterior, se adquirío un nuevo sistema de control ambiental para el cuarto de servidores. Además para el cuarto de principal de datos, se cumplió con la fecha de recarga del extintor. Mientras que para los cuartos de telecomunicaciones (Sótano, piso 1, piso 3 y piso 4) se etiquetó y ordenó el cableado. Adicionalmente, se efectuó una revisión de las medidas de seguridad física, la cual concluyó que todos los cuartos estaban debidamente asegurados.
Estado	Actualmente el cuarto principal de datos así como los cuartos de telecomunicaciones cuentan con medidas buenas de seguridad física y ambiental. Sin embargo todavía hay espacio para la mejora. Con respecto al cuarto principal, al cual se le puede adaptar un sistema de supresión de oxígeno. Y para los cuartos de servidores es aún posible integrar detectores de humo.

Hallazgo 05: Cumplimiento parcial de las actividades de respaldos y restauración. (4.2)	
Riesgo	Medio
Recomendación	A considerar que la definición, operación y monitoreo de un Sistema de Administración de la Seguridad de la Información (SI) tiene como propósito mantener el impacto y la frecuencia de incidentes relacionados a SI dentro del apetito de riesgo de la institución. La información sustraída del Sistema de Administración de la SI se usa como insumo para alimentar la matriz de riesgos de TI. Por lo tanto, con el fin disminuir el impacto de las actividades de un acceso no deseado a los sistemas del IMAS se sugiere: • Establecer un programa o cronograma de las actividades de respaldo y restauración junto con su respectivo control para garantizar la efectividad y la integridad de las actividades. Esta recomendación nace del hecho los riesgos que pudiesen llegar a materializarse por falta de actividades de respaldo o restauración de datos deberían tener controles asociados con el fin de minimizar el impacto de estos

Hallazgo 05: Cumplimiento parcial de las actividades de respaldos y restauración. (4.2)	
	riesgos. Es por esto que se considera que una solicitud puede solventar la necesidad de un respaldo o una restauración en ante un escenario determinado. Sim embargo un control preventivo es fundamental.
Acciones de Remediación	**Cumplido.** Con el propósito de cumplir con la recomendación del hallazgo, se procedió a eliminar las actividades relacionadas con antiguo Anexo 1: "Formulario de Bitácoras de Respaldo" y con el Anexo 2: "Formulario de Bitácoras de Pruebas" y se incluyo el "Formulario de Solicitud de Respaldo o Restauración de Datos" el cual se envía por medio de correo-e cuando se quiere llevar a cabo ejercicio de respaldo o restauración de datos.
Estado	Para la sección a: Se determinó que para la emisión 03 del documento, "Procedimientos para la Administración de respaldos y restauraciones de datos" se actualizó el proceso de solicitud de respaldos. Con el fin de completar una solicitud de esta naturaleza, es necesario completar el siguiente formulario: "Formulario de Registro de Pruebas o restauración", identificando temas como el nombre del solicitante, la unidad del solicitante, tipo de solicitud, motivos de la solicitud, fecha deseada, entre otras. Se cuenta con la evidencia. Se llevó a cabo un Para la sección b: Se determinó en el oficio "TI-163-07-2017 (coordinación Heredia sitio alterno)" quienes son los responsables del transporte de las cintas a Heredia. Además se establece una periodicidad mensual para la ejecución de esta actividad. El oficio fue recibido por la gerencia en Julio – 2017 y se cuenta con todas las bitácoras de la entrega de cintas en el sitio de Heredia desde Jun-2017 hasta Dic-2017.

Hallazgo 06: Oportunidades de mejora en el plan estratégico de TI. (2.1)	
Riesgo	Bajo
Recomendación	El interés por establecer buenas prácticas en la Administración de la estrategia es proporcionar un entendimiento holístico del actual ambiente tanto tecnológico como de negocios, la dirección futura y las iniciativas que servirán como impulsoras la transición entre el estado actual y el estado futuro de la institución. Todo esto con la intención de alinear los planes estratégicos de TI con las metas del negocio. Con respecto al estado actual del documento del Plan Estratégico de TI, a continuación las recomendaciones: • Elaborar un análisis de la situación actual tomando en consideración la evaluación del entendimiento de la estrategia de negocio, eficiencia de los procesos operativos y la aceptación de TI en la institución. • Establecer las acciones y actividades que van a contribuir a lograr los objetivos estratégicos identificados. • Definir una estructura organizacional del área junto con los roles y las responsabilidades de la misma.

Hallazgo 06: Oportunidades de mejora en el plan estratégico de TI. (2.1)	
	• Durante las reuniones del Comité Gerencial de TI darle prioridad y seguimiento a la revisión de los lineamientos del Plan Estratégico de TI (PETI) en relación con las metas del Plan Estratégico Institucional (PEI). El Plan Estratégico de TI de establecer de manera clara y detallada la estrategia del departamento de TI mediante la cual TI se va a integrar en la Misión, Visión y Objetivos estratégicos de la organización.
Acciones de Remediación	**Parcialmente cumplido.** Durante las reuniones trimestrales del Comité Gerencial de TI se le da un seguimiento al cumplimiento y a las actividades del área de TI con respecto al Plan Organizacional Gerencial (POGE) y no con respecto a Plan Estratégico de TI (PETI)
Estado	Luego de la revisión del Plan Estratégico de TI (PETI), se determinó que en relación con oportunidades de mejora propuestas por la auditoría anterior no se han tomado medidas correctivas sustanciales en la modificación del PETI.

Hallazgo 07: Deficiencias en el inventario de software del IMAS (4.2)	
Riesgo	Bajo
Recomendación	El manejo de las licencias de software forma parte del control de activos de la institución. Por lo tanto dentro las recomendaciones para este hallazgo están alineadas con las del hallazgo 10: "Cumplimiento parcial del procedimiento para el mantenimiento preventivo de Hardware y Software del I.M.A.S.".
Acciones de Remediación	**Cumplido.** Se remitió el oficio TI-112-05-2017 en el cual se solicita la desinstalación de las licencias de software excedentes.
Estado	Mediante el oficio TI-112-05-2017 se aclara la situación asociada a la falta de licencias del software DBArtisan, por lo cual se procede a solicitar la desinstalación del software. Sin embargo, dentro del oficio no se hace identifica el personal que tiene que acatar la orden. Tampoco se encuentra la documentación verificando que las licencias mencionadas fueron desinstaladas exitosamente. Sin embargo este fue un control correctivo que se aplicó para el hallazgo. Es clave contar con controles preventivos con el fin de disminuir la probabilidad e impacto que conlleva esta situación.

Hallazgo 08: Existencia de cuentas activas de exfuncionario en el Active Directory (AD) y base de datos. (1.4.5)	
Riesgo	Medio
Recomendación	A considerar que la definición, operación y monitoreo de un Sistema de Administración de la Seguridad de la Información (SI) tiene como propósito mantener el impacto y la frecuencia de incidentes relacionados a SI dentro del apetito de riesgo de la institución. La información sustraída del Sistema de Administración de la SI se usa como insumo para alimentar la matriz de riesgos de TI. Por lo tanto, con el fin disminuir el impacto de las actividades de un acceso no deseado a los sistemas del IMAS se sugiere: • Llevar a cabo una recertificación de usuarios con frecuencia anual/semestral para cada uno de los sistemas de la institución con el fin de asegurar que cada uno de sus funcionarios cuanta con los permisos de acceso correspondientes. • Fortalecer la comunicación con el área de Desarrollo Humano con el propósito de disminuir la probabilidad de que queden cuantas activas de los funcionarios que cesaron sus cargos.
Acciones de Remediación	**Cumplido.** Según el oficio TI-174-07-2017 se determinó que la verificación cruzada por parte del administrador de los sistemas con el personal de Desarrollo Humano entró en vigencia en Mayo del 2017.
Estado	Se remitió el oficio TI-174-07-2017 el cual hace referencia a la situación de las cuenta activas de exfuncionarios. Se documenta un recorrido por las pantallas tanto del Active Directory como las de SAP con el fin de verificar que el acceso y los permisos de cada uno de estos exfuncionarios han sido eliminados con éxito. Sin embargo este fue un control correctivo que se aplicó para el hallazgo. Es clave contar con controles preventivos con el fin de disminuir la probabilidad e impacto que conlleva esta situación.

Hallazgo 09: Debilidades en la implementación de cambios de los sistemas del IMAS. (3.2)	
Riesgo	Medio
Recomendación	La relevancia de la Administración de los cambios de forma controlada, es la habilitar la entrega de los servicios de negocio de forma rápida y confiable. Así mismo, para la mitigación del riesgo de impactos negativos hacia la estabilidad e integridad de los sistemas. A medida de recomendación lo siguiente: • El documento referente a los cambios establece las etapas a seguir a la hora de recibir una solicitud, las cuales son evaluar, priorizar y autorizar. • na vez que la solicitud está en ejecución se debe reportar y darle seguimiento a su estado. • Por último, una vez afianzado el cambio, junto con la aprobación del área interesada es necesario documentar los resultados.

Hallazgo 09: Debilidades en la implementación de cambios de los sistemas del IMAS. (3.2)	
	Se debe establecer un marco de referencia con el cual se pueda establecer una diferenciación clara entre Proyectos y Cambios. Con respecto a los proyectos, estos deben ser administrados y guiados por la oficina o encargado de proyectos de la institución. Mientras que los cambios van a ser atendidos por el departamento de soporte de TI haciendo diferencia cuando estos cambios van a ser desarrollados de forma interna o por medio de una subcontratación.
Acciones de Remediación	**Seguimiento.** El proceso de elaboración de los procedimientos para la atención de solicitudes de cambios y propuestas de nuevos proyectos está en curso. Se están analizando las metodologías posibles para disponer de un control y seguimiento tanto de los proyectos como de los cambios. Actualmente el departamento de TI está llevando a cabo la planificación para determinar la separación entre proyectos y cambios así como de la identificación de los roles y las responsabilidades para cada uno de estos.
Estado	Actualmente, a nivel de políticas y procedimientos no se hace una distinción entre solicitudes de cambios (implementación y mantenimiento) y nuevos proyectos. Dependiendo de la magnitud de esta solicitud, se va a categorizar como un cambio o un proyecto. Actualmente no se hace una distinción entre los proyectos y los cambios. Por este motivo. Hay un procedimiento en el cual se detallan cuáles son las etapas de un proyecto y como darle seguimiento. Mientras que no se cuenta con un documento que aclare que se considera como un cambio. Ante esta situación todas las solicitudes de cambio o de implementación que llegan al departamento de TI no se les pueden dar un correcto seguimiento y control. Es importante aclarar que este procedimiento/documento no aplica para todos los desarrollos que se llevan a cabo por parte del equipo de TI del IMAS. Además es necesario aclara bien la diferencia entre los proyectos y los desarrollos (solicitudes o mantenimiento). Con respecto a la segregación de ambientes en el sistema de recursos humanos no se cuenta con pruebas para el código fuente, el cual si es modificado constantemente.

Hallazgo 10: Cumplimiento parcial del procedimiento para el mantenimiento preventivo de hardware y software del IMAS. (4.2-d)	
Riesgo	Bajo
Recomendación	La relevancia establecer un proceso de Administración de activos es la contabilidad de los mismos con el fin de optimizar su valor a un costo óptimo. Esta Administración de los activos debe residir a lo largo de todo su ciclo de vida, tomando en cuenta su seguridad física. Y para los activos críticos que soportan la capacidad de los servicios deben ser confiables y estar disponibles en todo momento. Como parte de las recomendaciones, se decreta lo siguiente: • Mantener un registro actualizado y preciso de todos los activos requeridos para la entrega de servicios.

Hallazgo 10: Cumplimiento parcial del procedimiento para el mantenimiento preventivo de hardware y software del IMAS. (4.2-d)	
	• Llevar a cabo revisiones del inventario de estos activos periódicamente con el fin de instaurar nuevas formas de optimizar los costos y mantener el lineamiento con las necesidades de negocio así como tener un panorama institucional del estado de los activos tecnológicos que impulsan la estrategia de negocio. • Elaborar las bitácoras de revisión de los activos especificando cuales fueron los activos revisados al igual que las actividades realizadas con el objetivo de asegurar la integridad de las revisiones.
Acciones de Remediación	**Parcialmente cumplido.** Mediante el oficio TI-010-01-2018 se determina el cronograma de visitas a los diferentes centros del IMAS con el fin de darle el mantenimiento preventivo adecuado a los sistemas críticos.
Estado	Al día de hoy, las actividades de mantenimiento preventivo se pueden establecer de dos formas. La primera es por medio de una solicitud de la mesa de servicio. Y la segunda es mediante el cronograma de mantenimiento de equipo crítico, establecido en el oficio TI-010-01-2018. Con respecto a las solicitudes de mantenimiento de equipo que se hacen por medio de la mesa de servicio, a la hora de la revisión no se cuenta con un mecanismo que asocie la solicitud del sistema con el vale físico de la revisión. Por lo que no se le puede dar un seguimiento apropiado al mantenimiento. No en todos los casos se detallan las actividades específicas que se llevaron a cabo a la hora de la revisión. Lo cual dificulta el seguimiento al mantenimiento de los equipos por falta de un sistema de control de mantenimiento del equipo institucional. A pesar de que se elaboró el cronograma para el mantenimiento preventivo de los equipos críticos no se cuenta con un control o seguimiento de las actividades que detallen tanto la actividad como el equipo involucrado. Como resultado de no llevar un control de la mano con mesa de servicio reduce la posibilidad de identificar problemas basado en el análisis de incidentes, que se usa como insumo para la actualización de la matriz de riesgos basado en los problemas e incidentes detectados. Con respecto a los activos, es importante tenerlos bien categorizados ya que los activos críticos deberían contar con un programa de mantenimiento al menos anual. Finalmente, el oficio TI-010-01-2018 fue remitido en enero del 2018 por lo tanto no fue posible comprobar su efectividad en el periodo de la auditoría en curso.

Hallazgo 11: Deficiencias en la gestión de calidad de los productos y servicios de TI. (1.2)	
Riesgo	Bajo
Recomendación	La importancia de tener un control confiable y estructurado de la calidad es asegurar que los productos y los servicios ofrecidos por TI alcancen los requerimientos de calidad de manera consistente con el fin de satisfacer las necesidades de los encargados de las áreas interesadas. Con respecto a las recomendaciones, es importante: • Elaborar el catalogo que contenga la totalidad de los productos y servicios de TI. Este trabajo debe llevarse a cabo con la participación de todas las Jefaturas de la institución. • Analizar la naturaleza de cada uno de los elementos del catálogo de servicios y de productos con el fin de establecer las métricas de rendimiento con las cuales se van a evaluar. Es recomendable establecerlo mediante políticas y procedimientos. • Llevar a cabo programa de monitoreo, control y revisiones de la calidad de los productos y servicios.
Acciones de Remediación	**Seguimiento.** El oficio TI-340-12-2017, aclara la situación donde recientemente el documento P-EDI-02 que hacía referencia al control de la calidad fue modificado y actualmente hace referencia a otro proceso. Además se estableció un cronograma para la remediación de este hallazgo, el cual ya pasó por una revisión por parte del departamento de Planificación y actualmente están en vísperas de la formulación de un procedimiento que esté acorde con el cumplimiento.
Estado	Actualmente, no se cuenta un procedimiento formal de gestión de la calidad para los productos y servicios de TI. Tomando como referencia el documento PI-106-04-2018 que es la respuesta de parte del área de Planificación Institucional hacía TI, se responde a la solicitud por parte de TI de valorar el establecimiento de un sistema de calidad para los productos y servicios de TI, a la cual se responde con lo siguiente: • Un breve análisis acerca de los beneficios que implica contar con un control de calidad de los productos y los servicios a nivel institucional con el fin de poder analizar esta información y utilizarla para el crecimiento y desarrollo de la institución. • Una solicitud listando cuales son los productos y servicios de TI que van a ser evaluados mediante este sistema. • Así como estructura de las métricas que van a ser utilizadas para medir estos productos y servicios. Dentro de los plazos de cumplimiento establecidos para los hallazgos de la auditoría del 2016 se establece que la fecha límite de resolución de este hallazgo es en Noviembre del 2019.

Hallazgo 12: Cumplimiento parcial del plan de compras de hardware y software. (4.2-h)	
Riesgo	Bajo
Recomendación	Con el fin de fomentar la relación entre TI y las demás áreas de la institución es fundamental impulsar la eficiencia y la efectividad del uso y adquisición de los recursos tecnológicos así como promover la transparencia y la responsabilidad del costo y el valor de los mismos. Para lograr esto es necesario establecer un presupuesto que refleje las prioridades de inversión en relación con los objetivos estratégicos de la institución. Para garantizar el cumplimiento preciso. Recomendaciones para cumplir con el plan de compras: • Establecer un plan de seguimiento periódico para garantizar el cumplimiento.
Acciones de Remediación	**Parcialmente cumplido.** En relación con el hallazgo de la auditoría del año 2016, la Jefatura de TI señalo que el incumplimiento del plan de compras fue un resultado de la falta de comunicación entre las áreas y que el equipo no adquirido no formaba parte del plan de compras de TI. Se hace referencia al oficio TI-193-08-2017 en el cual se cumple con una de las recomendaciones de la auditoría anterior. Esta recomendación dicta la responsabilidad por parte de las áreas de la institución de notificar proactivamente a Proveeduría en caso de que se identifiquen nuevas necesidades o bien los motivos por los cuales no se llevaron a cabo las compras. Adicionalmente se remite la circular CG-1616-08-2017 en la cual se les recuerda a todos los funcionarios del I.M.A.S. lo establecido en el oficio TI-193-08-2017.
Estado	Actualmente, no se le da un seguimiento que incluya el control y monitoreo continuo al plan de compras de las áreas del I.M.A.S. Una vez que cada área hace la solicitud, esta pasa por un proceso dentro del departamento de presupuesto con el fin de analizar la justificación de dicho presupuesto en relación con la dirección estratégica de la institución. Cada una de las áreas es responsable de llevar a cabo la proyección de sus necesidades para el año posterior. Sin embargo en relación con los recursos relacionados a TI, se establece informalmente que el área de tecnología es responsable de consolidar las necesidades de los recursos tecnológicos de todas áreas para incluirlo dentro de su presupuesto. El conflicto con la situación anterior es que las áreas interesadas no informan al área de TI acerca del seguimiento y cumplimiento de su equipo tecnológico. Por lo tanto, si una de estas áreas no cumple a cabalidad con la ejecución del presupuesto, esto se va a ver reflejado como una deficiencia dentro del área de TI debido a que esta incluyó los recursos dentro de su proyección. Más aún, durante el periodo de la auditoría se tuvo acceso al plan de compras del departamento de TI, debidamente firmado y aprobado. Sin embargo lo que no se pudo evidenciar fue el documento que consolida las necesidades de compra de recursos tecnológicos de todas las áreas de la institución.

Hallazgo 13: Cumplimiento parcial del plan de capacitaciones para los funcionarios de TI del IMAS. (2.4)	
Riesgo	Medio
Recomendación	La importancia de una buena Administración de los recursos humanos es suministrar un acercamiento que sea capaz de asegurar una estructuración óptima, acomodamiento, derecho a las decisiones y las calificaciones del personal. Para lograr lo anterior, es indispensable la comunicación de los roles y las responsabilidades del puesto, planes de aprendizaje y crecimiento y el desempeño esperado en la institución. Como recomendación, es necesario: • Establecer un programa anual de capacitación aprobado por el Comité Gerencia de TI. • El programa debe tener como objetivo contar con personal más capacitado con el fin de contribuir en el cumplimiento de las metas de negocio.
Acciones de Remediación	**Parcialmente cumplido.** Para el año 2007, la capacitación de inducción es un documento enviado por medio de correo electrónico en el cual se incluyen los credenciales siguientes: • De ingreso al dominio del I.M.A.S. • De ingreso al correo electrónico. • De ingreso al sistema de Desarrollo Humano. • Para registrar asistencia y puntualidad. En caso de que el funcionario ocupase acceso adicional a un sistema del IMAS es necesario coordinar con la Jefatura correspondiente.
Estado	Con respecto al año 2017, se determinó que no se llevó a cabo un plan de capacitación para el personal de TI. La elaboración del plan de capacitación se hace en conjunto entre el área que va a recibir la capacitación y el área de DH. El área involucrada tiene como objetivo identificar las necesidades del departamento para contribuir a la confección del programa de capacitación.

Erick Brenes F.
Socio
T +506 2201-4130
E erickbrenes@kpmg.com

Luis Rivera
Director
T +506 2201-4130
E lgrivera@kpmg.com

Otto Mora
Supervisor
T +506 2201-4130
E ottomora@kpmg.com

KPMG Costa Rica
Edificio KPMG
Boulevard Multiplaza
San Rafael de Escazú, Costa Rica
T +506 2201- 4100
kpmg.co.cr