San José, 19 de agosto de 2022.
MIVAH-AI-0076-2022

Sra. Lilliana Reyes Piña
Jefa Departamento de Tecnología e Información (DTIC)
Ministerio de Vivienda y Asentamientos Humanos

Asunto: Respuesta a su oficio MIVAH-DVMVAH-DTIC-0074-2022, originado según oficio de la Contraloría General de la República (DFOE-CAP-2264 del 01/08/2022).

Estimada señora:

En respuesta al oficio de cita y considerando el oficio emitido por la Contraloría General de la República (CGR) en relación con la "Aplicación de prácticas de seguridad de la información en las instituciones públicas" es que valoramos sus consultas, para detallar algunos aspectos de nuestra gestión diaria, adicionalmente, para aclarar los roles y funcionalidad de Auditoría Interna con respecto a la "Administración Activa".

Así mismo, se considera conveniente asesorar y advertir[1] a los Jerarcas del MIVAH para que se analicen los aspectos consultados por CGR con prontitud y de manera **planificada institucionalmente**, lo anterior, con base a la Ley General de Control Interno (LGCI), sus normas y como se menciona en el oficio de la CGR en cumplimiento de las medidas técnicas que emite el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). En dichas normas técnicas, se detalla el papel de la Unidad o Departamento de Tecnologías de Información y Comunicación y de la Dirección de Planificación Institucional para gestionar una instancia de alto nivel con las autoridades de la institución, estableciendo un espacio de diálogo y coordinación en temas como lo son Gobernanza de TI, seguridad y ciberseguridad.

Procedo a dar respuesta a sus consultas en el orden normal de las mismas:

1. **¿Cuenta su Dirección o Unidad con un Plan de Continuidad del Negocio?**

Existe un compendio de procedimientos de Auditoría Interna del MIVAH producto de la atención de nuestras labores en acatamiento de la LGCI, las Normas de Control Interno y las Normas Generales de Auditoría; dichos procedimientos abarcan en su conjunto cada una de las 4 fases (planificación, ejecución, comunicación y seguimiento) que componen la gestión de Auditoría. Estos documentos detallan las actividades a realizar para efectos de la herramienta automatizada AUDINET Planning y en caso de que el servicio de dicha herramienta se interrumpa, se cuenta con procedimientos formalizados en formato PDF, garantizando así la continuidad del negocio ***(Procedimientos AI.03.02.01, AI.03.02.02, AI.03.02.03 y AI.03.02.04).***

2. **¿Dispone su Dirección o Unidad de un estudio de impacto sobre el funcionamiento en caso de materializarse un riesgo con la pérdida de activos de información?**

[1] LGC, Artículo no.22 Competencias Asesorar, en materia de su competencia, al jerarca del cual depende; además, advertir a los órganos pasivos que fiscaliza sobre las posibles consecuencias de determinadas conductas o decisiones, cuando sean de su conocimiento.

Se cuenta con 4 diferentes repositorios de información: sistema AUDINET Planning, oficial y especializado para funciones de Auditoría Interna en todas sus fases (planificación, ejecución, comunicación y seguimiento) resguardo de la información en "carpetas compartidas" "z", "j" y "y" donde se replica la información de los estudios de Auditoría Interna y su correspondencia oficial (con firma digital desde 2019), adicionalmente, existe un blog de publicación de informes en la Web e Intranet del MIVAH, como medios oficiales para la divulgación de los productos finales de la Auditoría Interna.

El impacto mencionado en la consulta es mitigado (función preventiva y detectiva) según los procedimientos de la pregunta uno y los repositorios de información ya citados. Al respecto, se debe indicar que hasta el día de hoy no se ha materializado ninguna pérdida de activos (no existen eventos o incidentes históricos) de información de la Auditoría Interna del MIVAH, por lo tanto, la probabilidad e impacto calculada es baja o mínima, no obstante, el objetivo de la consulta de CGR no es para Auditoría Interna sino para la Administración Activa según LGCI.

3. ¿Ha establecido e implementado su Dirección o Unidad mecanismos para la identificación de desviaciones conforme a la "tolerancia – límite de riesgo" definido como aceptable?

En cuanto a seguridad de información, únicamente los funcionarios de la Auditoría Interna del MIVAH tienen un usuario y clave de acceso para AUDINET Planning y en lo que respecta a las "carpetas compartidas" detalladas en la pregunta anterior, solamente los mismos funcionarios de Auditoría Interna son los que pueden ingresar a estos repositorios de información según se ha coordinado con el DTIC del MIVAH.

En resumen, no se determinan desviaciones de riesgo porque con estas gestiones se cumple la normativa vigente que rige el accionar de las Auditorías Internas del Sector Público.

Se aclara que los análisis de riesgos[2] y su nivel de tolerancia son aspectos técnicos que la Administración Activa del MIVAH, debe aplicar a sus procesos según LGCI y no fueron diseñados técnicamente para fines de la labor diaria que debe realizar la Auditoría Interna.

El análisis de riesgo que sí efectúa la Auditoría Interna y que consta en cada uno de sus estudios en AUDINET Planning, es el que realizamos para fines de la fijación de prioridades en la fundamentación del plan de pruebas de Auditoría, en conclusión, es otro el objetivo

[2] Artículo 14. —**Valoración del riesgo**. En relación con la valoración del riesgo, serán deberes **del jerarca y los titulares subordinados**, entre otros, los siguientes: a) **Identificar y analizar los riesgos** relevantes asociados al logro de los objetivos y las metas institucionales, definidos tanto en los planes anuales operativos como en los planes de mediano y de largo plazos. b) Analizar el efecto posible de los riesgos identificados, su importancia y la probabilidad de que ocurran, y decidir las acciones que se tomarán para administrarlos. c) Adoptar las medidas necesarias para el funcionamiento adecuado del sistema de valoración del riesgo y para ubicarse por lo menos en un nivel de riesgo organizacional aceptable) Establecer los mecanismos operativos que minimicen el riesgo en las acciones por ejecutar.

que se persigue cuando se habla de los análisis de riesgos que elabora la Auditoría Interna según nuestras competencias otorgadas por la LGCI.

4. ¿Su Dirección o Unidad ha integrado la seguridad de la información a los distintos procesos que ejecutan?

Cabe indicar que la función de la Auditoría Interna se rige en lo que respecta al manejo y seguridad de información según lo determinado por la LGCI en su **Artículo 32 Deberes, potestades y prohibiciones de los funcionarios de auditoría** y en las **Normas Generales de Auditoría para el Sector Público** se define en el **Capítulo I Normas Personales**: 101. Independencia y objetividad 102. Impedimentos a la independencia y objetividad 103. Naturaleza confidencial y discreción sobre el trabajo 104. Ética profesional 105. Competencia y pericia profesional y 106. Debido cuidado profesional.

5. ¿La Dirección o Unidad ha instruido a su personal acerca del comportamiento esperado en procesos de recolección y manejo de información sensible o crítica?

Como se indicó en la consulta No.4 existen aspectos normativos que rigen el quehacer de una Auditoría Interna del Sector Público, para ahondar aún más en el tema y al invocar las **Normas Personales** según las **Normas Generales de Auditoría para el Sector Público**, procedemos a detallar algunas de ellas para referencia de su consulta:

> ***"…101. Independencia y Objetividad: El personal que ejecuta el proceso de auditoría en el sector público debe mantener un criterio independiente en el desarrollo de su trabajo, y actuar de manera objetiva, profesional e imparcial.***
>
> ***103. Naturaleza confidencial y discreción sobre el trabajo: Durante la ejecución de la auditoría los papeles de trabajo son de acceso restringido, por lo que el personal que participa en el proceso de auditoría en el sector público debe mantener reserva y la discreción debida respecto de la información obtenida durante el proceso de auditoría, y no deberá revelarla a terceros, salvo para los efectos de cumplir con requerimientos de las instancias públicas autorizadas legalmente.***
>
> ***106. Debido cuidado profesional: El personal que participa en el proceso de auditoría en el sector público debe ejecutar siempre sus funciones con el debido cuidado, pericia y juicio profesional, con apego a la normativa legal y técnica aplicable y a los procedimientos e instrucciones pertinentes de su organización de auditoría.***
>
> ***El equipo de auditoría debe aplicar su juicio profesional para tomar las decisiones de auditoría, debidamente razonadas y documentadas, durante las distintas actividades del proceso; (planificación, examen, comunicación de resultados y seguimiento), por lo que debe valorar aspectos como el costo beneficio de las acciones, el riesgo de auditoría, la importancia relativa, la materialidad y la evidencia disponible al momento de tomar la decisión.***

El juicio profesional debe ser aplicado a las circunstancias de la auditoría, de acuerdo con el conocimiento, competencia profesional y experticia de los auditores. La aplicación del juicio profesional debe estar enmarcada dentro de los siguientes parámetros:

a) Ajustarse a la debida diligencia profesional.
b) Alinearse con el ordenamiento jurídico y técnico aplicable.
c) Tener en consideración los objetivos de la auditoría…" (Lo resaltado y subrayado no es del original)

6. ¿Se encuentran identificados los procesos críticos de la gestión de su Dirección o Unidad?

No existen procesos críticos desde la gestión de Auditoría Interna, existen competencias, labores y servicios "técnicos" y están definidas por:

a) De manera primordial según LGCI en su **Artículo No. 22 Competencias**.
b) Tipos de Auditoría (financiera, operativa o de carácter especial) que se detallan en las Normas de Auditoría para el Sector Público.
c) Los servicios de Auditoría según el Manual de Normas para el Ejercicio de la Auditoría del Sector Público (servicios de asesoría, atención de denuncias, advertencias y autorización de libros)

Razón por la cual, todos los flujos de información obtenidos u originados de estas labores son tratados de la misma manera y en apego de los aspectos normativos que se indicaron en las consultas No.4 y No.5.

7. ¿Se ha identificado y clasificado la información crítica y/o sensible que accede o genera su Dirección o Unidad?

Se repite la misma respuesta de la consulta No.6.

8. ¿Considera que estas preguntas generan algún aprendizaje para la adecuada gestión de su Dirección o Unidad? Detalle.

Se indica que el origen de la consulta planteada por la CGR (DFOE-CAP-2264 de 01 de agosto de 2022) es hacia los Jerarcas, es decir, a la "Administración Activa" y se copió a las Auditores Internos **(nuestro rol es verificar que se envíe oportunamente la información a CGR**), es por ello que, al ser la función[3] de la Auditoría Interna una actividad independiente, objetiva y asesora no vemos necesario que este tipo consultas sean dirigidas a la Auditoría Interna debido a que el ente Contralor, es el emisor del espectro normativo que determina el actuar de las Auditoría Internas del Sector Público

[3] **LGCI. Artículo 21.-Concepto funcional de auditoría interna.** La auditoría interna es la actividad independiente, objetiva y asesora, que proporciona seguridad al ente u órgano, puesto que se crea para validar y mejorar sus operaciones. Contribuye a que se alcancen los objetivos institucionales, mediante la práctica de un enfoque sistémico y profesional para evaluar y mejorar la efectividad de la administración del riesgo, del control y de los procesos de dirección en las entidades y los órganos sujetos a esta Ley. Dentro de una organización, la auditoría interna proporciona a la ciudadanía una garantía razonable de que la actuación del jerarca y la del resto, de la administración se ejecuta conforme al marco legal y técnico y a las prácticas sanas.

en todas sus fases, competencias y debida diligencia (esto incluye los activos de información).

Se debe tener claro los roles y alcances de los integrantes del sistema de control interno según LGCI, ya que la Auditorías Internas **no** son "Administración Activa":

> ***Artículo 9º—Órganos del sistema de control interno. La administración activa y la auditoría interna de los entes y órganos sujetos a esta Ley serán los componentes orgánicos del sistema de control interno establecido e integrarán el Sistema de Fiscalización Superior de la Hacienda Pública a que se refiere la Ley Orgánica de la Contraloría General de la República.***
>
> ***Artículo 10. —Responsabilidad por el sistema de control interno. Serán responsabilidad del jerarca y del titular subordinado establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional. Asimismo, será responsabilidad de la administración activa realizar las acciones necesarias para garantizar su efectivo funcionamiento.***

A partir de esta consulta y de acuerdo con nuestras competencias, se observa la relevancia de abarcar estos temas que son parte de la "gobernanza de TI" **(Normas técnicas para la gestión y el control de las Tecnologías de Información)** y que son materias para desarrollar por parte de la "Administración Activa", dentro de los ejes de planificación estratégica y planes anuales operativos según el tamaño o la complejidad de las labores diarias del MIVAH. Estos aspectos deben ser orientados a lo interno del Ministerio por los órganos rectores y colegiados que define claramente la citada norma.

Por otra parte, los aspectos tratados en la consulta de la CGR deben ser revisados para determinar los grados de "madurez" alcanzados por la entidad en el desarrollo de estos a lo largo del tiempo.

A raíz de esta comunicación planteada por la CGR, del oficio del DTIC y en virtud de nuestras competencias para **asesorar y advertir** a la Administración Activa, por parte de la Auditoría Interna se considera necesario que se revisen a lo interno del MIVAH los siguientes aspectos de las normas de control interno:

Capítulo IV: Normas sobre Actividades de Control**:**

> ***"…4.4.1 Documentación y registro de la gestión institucional***
> *El jerarca y los titulares subordinados, según sus competencias, deben establecer las medidas pertinentes para que los actos de la gestión institucional, sus resultados y otros eventos relevantes, se registren y documenten en el lapso adecuado y conveniente, y se garanticen razonablemente la* ***confidencialidad*** *y el acceso a la información pública, según corresponda.* (lo resaltado y subrayado no pertenece al original)
>
> ***5.7.4 Seguridad***
> *Deben instaurarse los controles que aseguren que la información que se comunica resguarde sus características propias de calidad, y sea trasladada bajo las condiciones de protección apropiadas,* ***según su grado de sensibilidad y***

> ***confidencialidad****. Así también, que garanticen razonablemente su disponibilidad y acceso por parte de los distintos usuarios en la oportunidad y con la prontitud que la requieran.* (lo resaltado y subrayado no pertenece al original).

Así mismo en su capítulo Capítulo V: Normas Sobre Sistemas de Información establece:

> ***5.8 Control de sistemas de información***
> *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****.* (lo resaltado y subrayado no pertenece al original)

Por otra parte, en las normas de Control Interno del Sector Público y normas COSO, en relación con lo indicado por la Ley General del Control Interno indican de manera específica**:**

> ***"…5.7.1 Canales y medios de comunicación***
> *Deben establecerse y funcionar adecuados canales y medios de comunicación, que permitan trasladar la información de manera transparente, ágil, segura, correcta y oportuna,* ***a los destinatarios idóneos dentro y fuera de la institución****.* (lo resaltado y subrayado no pertenece al original)
>
> ***5.7.2 Destinatarios***
> *La información debe comunicarse a las instancias competentes, dentro* ***y fuera de la institución, para actuar con base en ella en el logro de los objetivos institucionales…"*** (lo resaltado y subrayado no pertenece al original)

Me despido atentamente.

OLDEMAR HERNANDEZ AULD (FIRMA)

Firmado digitalmente por OLDEMAR HERNANDEZ AULD (FIRMA)
Fecha: 2022.08.19 14:08:12 -06'00'

Lic. Oldemar Hernández Auld. CPA.
Auditor Interno, MIVAH.

Sr. Jéssica Martínez Porras. Ministra. Ministerio de Vivienda y Asentamientos Humanos
Sr. Roy Allan Jiménez Céspedes. Viceministro. Ministerio de Vivienda y Asentamientos Humanos
Sr. Abelardo Quirós Rojas. Jefe. Unidad de Planificación Institucional.
Sra. Yolanda González Castro, Directora DAF con recargo de Jefatura de Despacho Ministerial.
Archivo.