MSP-DM-AG-01-792-2018
21 de julio de 2018

Señor
Michael Soto Rojas
Ministro

Asunto: Documento de advertencia 01-057-2018 AD/TI, sobre riesgos relacionados con la Seguridad de la Información Institucional.

Estimado señor:

Como parte del servicio de "advertencia" que nos compete efectuar y en vista del interés permanente de esta Auditoría General por el mejoramiento continuo de los procesos y sus productos, reviste particular importancia referirnos al tema de los riesgos relacionados con la Seguridad de la Información Institucional.

Con fundamento en el análisis de eventos propios del quehacer institucional, comunicaciones en diferentes medios internos y externos, y la Matriz de Formulación de Riesgos 2018 del Ministerio; se procedió a revisar la normativa vigente en esta materia, determinándose que existen inconsistencias relevantes de control interno que son susceptibles de mejora apremiante.

Dadas las características propias de las operaciones de nuestro Ministerio, resulta necesario en primer término rescatar lo establecido en el artículo 17 de la Ley 7530 de Armas y Explosivos, sobre el control de armas en poder del Estado, que establece lo siguiente:

> *"La Dirección [General de Armamento] llevará un control estricto de las armas en poder del Estado y sus instituciones. Elaborará un inventario permanente de esas armas y enviará un informe anual a la Auditoría del Ministerio. Los informes remitidos, únicamente, podrán ser conocidos cuando medie el interés público".*

Si bien con el artículo 39 de la Ley N° 8823 del 5 de mayo de 2010[1], se excluyó la

[1] Ley de Reforma de Varias Leyes sobre la Participación de la Contraloría General de la República para la Simplificación y el Fortalecimiento de la Gestión Pública (N° 8823)

palabra confidencial de este párrafo, el carácter de información reservada de los asuntos relacionados con armas se mantiene tácitamente en la última oración de ese artículo. Además, la clasificación de confidencialidad se mantiene en el artículo 11 de la misma Ley que dispone lo siguiente:

> *"La Dirección [General de Armamento] estará integrada por el Departamento de Control de Armas y Explosivos, el Registro de Armas y el Arsenal Nacional.*
>
> *El Registro de Armas será confidencial y solo tendrán acceso a él las autoridades administrativas y judiciales competentes".*

Es preciso mencionar que, los datos relacionados con armas en poder del Estado constituyen el principal activo de información en el Ministerio, a nivel institucional se genera información que puede considerarse restringida, como por ejemplo: bases de datos, archivos y registros de armerías, operatividad policial, seguridad para expresidentes, recursos humanos, tecnologías de Información, prensa, informes de auditoría y gran cantidad de documentación relacionada con el quehacer Institucional.

No obstante lo comentado, el documento de riesgos formulados por las diferentes instancias del Ministerio para el año 2018, deja entrever que solamente 8 de 108 riesgos están relacionados con seguridad de la información (Tabla 1 adjunta); lo cual resulta una proporción sumamente baja, ante las características de los objetivos estratégicos en materia de seguridad ciudadana.

Los funcionarios involucrados en este proceso probablemente no han formulado (y por ende es posible que no hayan identificado) riesgos comunes de seguridad de la información como: fuga de datos, fraude y robo, alteración o modificación de información oficial, divulgación no autorizada, uso indebido de códigos de usuarios, suplantación de identidad, divulgación de contraseñas, eliminación inadecuada de medios (papel, discos, dispositivos USB y otros), y acceso no autorizado de funcionarios a oficinas o áreas que contienen información confidencial.

Dado lo anterior y con base en el concepto de confidencialidad, esta Auditoría General advierte sobre la urgencia de llevar a cabo una revisión integral de los controles actuales sobre las fuentes de datos internas, su manipulación o procesamiento computadorizado, y sobre todo del proceso de publicación de la información resultante, tanto en el ámbito interno como el externo al Ministerio; todo esto en coincidencia con las funciones propias del Ministerio y la noción de interés público.

Para mejor comprensión, la Sala Constitucional mediante resolución 517-98, del 26 de agosto de 1998, precisó un punto de partida para la actividad interna de catalogar los tipos de datos que se administran en la Institución, y la conveniencia de su publicación:

> *La determinación de si una necesidad es de interés público no es una cuestión jurídica, sino de hecho y circunstancial, que obliga –como ya se dijo- a un juicio de oportunidad y conveniencia. No existen actividades que por "naturaleza" o imperativos del Derecho Constitucional sean propias del servicio público, sino que eso dependerá de cada sociedad, sus necesidades y en el ámbito –privado o público- en que estas se satisfagan de mejor manera...".*

Por lo anterior, este Órgano Fiscalizador sugiere que se implementen a la brevedad posible políticas y procedimientos para la Seguridad de la Información, en los cuales se clasifique clara y oficialmente la información que se procesa en la Institución, los responsables de su custodia y divulgación al país, en los diferentes formatos como son: electrónico, digital, impreso, audio y vídeo.

En materia de seguridad de la información el estándar internacional ISO 27001 y su guía de aplicación ISO 27013 (provistos en Costa Rica por el Instituto de Normas Técnicas de Costa Rica, INTECO) brindan una metodología para seleccionar adecuadamente las políticas y controles que permitan contar con certeza razonable sobre el procesamiento y la publicación de la información, de tal manera que no se materialicen riesgos en la seguridad nacional, la imagen institucional, la seguridad interna del Ministerio, y el logro de los objetivos institucionales.

En concordancia con la norma 5.1.1 del citado estándar, los esfuerzos deben iniciarse con la documentación oficial de políticas de seguridad que provean dirección gerencial y apoyo efectivo a las instancias administrativas involucradas en materia de seguridad de la información. La norma 5.1.2 sobre revisión de las políticas de seguridad, indica que esa documentación debe revisarse permanentemente para asegurar la continua idoneidad, eficiencia y efectividad de este proceso.

Por otra parte, la norma 6.1.3 especifica que se deben asignar claramente las personas responsables de proteger los activos de información y las responsabilidades inherentes de sus cargos. La norma 6.1.5 sobre acuerdos de confidencialidad, explica que se deben identificar, oficializar y revisar permanentemente los requerimientos de confidencialidad, y acuerdos de no divulgación de la información por parte de los colaboradores responsables.

Una de las más importantes para el tema en discusión es la norma 7.2.1 sobre lineamientos de clasificación, la cual establece que la información debe clasificarse en términos de su valor, requisitos legales, tipo de confidencialidad y criticidad según su naturaleza. Una jerarquía de información generalmente aceptada es: interna, pública, restringida, reservada o confidencial.

En resumen, el carácter confidencial o reservado de los datos de armas en poder del Estado y su control, así como otra documentación que se determine como sensible, debe transferirse a la documentación oficial que se genere de las operaciones diarias; y además a su perímetro lógico (sistemas computacionales) y físico (instalaciones centrales y regionales donde se mantengan o custodien activos de información). Para esto se requiere un trabajo interdisciplinario de análisis detallado de datos y responsables, que clasifique eficazmente los datos, medios y responsables de brindar la información a la ciudadanía y entidades externas interesadas.

Por tanto, en atención a lo dispuesto en el artículo 12, incisos b y c, de la Ley General de Control Interno (N° 8292) y en aras de coadyuvar con el mejoramiento del control y el logro de los objetivos institucionales, se considera urgente que la Administración encargada proceda con la implementación de un sistema de gestión permanente de seguridad de la información, el cual brinde lineamientos efectivos y dirija las actividades de recopilación, análisis, procesamiento, toma de decisiones y publicación de los datos del Ministerio, en relación con los riesgos comentados en este documento.

Por último, sírvase comunicar a esta Auditoría General, mediante el Sistema de Gestión de Informes, sobre las acciones que se emprendan para la eficaz atención de los temas supra citados.

Atentamente,

DOUGLAS EDUARDO ELIOTH MARTINEZ (FIRMA)

Digitally signed by DOUGLAS EDUARDO ELIOTH MARTINEZ (FIRMA)
Date: 2018.08.21 15:19:20 -06:00
Reason: Aprobado
Location: Costa Rica, San Jose, San Jose, Carmen

Douglas Elioth Martínez
AUDITOR INTERNO

Anexo: Tabla 1 sobre riesgos formulados en relación con la seguridad de la información
maav
C:

Tabla 1
Riesgos relacionados con seguridad de la información del Ministerio de Seguridad Pública según SEVRI 2018

Riesgo	Instancia	Evento	Riesgo inherente	Riesgo esperado
DGA-04-2016	Dir. General de Armamento	La posibilidad de filtraciones e incursiones de personas o individuos del crimen común u organizado en las instalaciones de la Dirección General de Armamento y sus Departamentos, viabilizando eventuales daños y hasta posibles pérdidas de bienes, información y vidas humanas	Muy Alto	Muy bajo
ENP-001-2018	Escuela Nacional de Policía	Probabilidad de pérdida de información digital y documental al no contar con el mantenimiento y actualización del Sistema de Registro y los espacios adecuados para el archivo de los expedientes académicos de los procesos educativos policiales	Medio	Muy Bajo
DTI-002-2017	Dir. Tecnologias de Información	Posibilidad de pérdida y no recuperación de información estratégica y operativa loalizada en los sistemas de información y bases de datos de la institución	Medio	Medio
DTI-001-2017	Dir. Tecnologias de Información	Posibilidad de acceso no autorizado a las bases de datos y sistemas de información sensible de la institución	Muy Alto	Medio
DAL-03-2018	Dir. Apoyo Legal Policial	"Probabilidad de no garantizar una eficiente prestación del servicio por parte de los asesores legales de DALEP, en tiempo real y con el soporte tecnológico adecuado."	Muy Bajo	Muy Bajo
DGFP-001-2018	Dir. General de la Fuerza Pública	Inexistencia de información oportuna que permita la toma de decisiones ágil por parte de los titulares subordinados con relación a la implementación de su planificación interna (gestión operativa y gestión administrativa)	Alto	Muy Bajo
DPI-002-2018	Dir. Proveeduría Institucional	Posibilidad de que la información que se consultará, sea hallada de manera incompleta para el procedimiento de contratación administrativa, seguido por esta Dirección	Alto	Bajo
DFP-02-2016	Dir. Financiera	La probabilidad de no contar con la información interna por parte de los centros gestores de las circunstancias presentadas con respecto a la ejecución de los recursos	Alto	Medio

Fuente: datos de la Matriz Institucional de Formulación de Riesgos 2018, suministrada por la Oficina de Mejoramiento y Control mediante correo electrónico del 24/JUL/2018