INFORME EJECUTIVO DE AUDITORÍA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES – TIC	Número ID	ASEG-07
	Fecha	19-10-2018

I. CONTEXTO

1. Materia: Tecnologías de Información y Comunicaciones.
2. Alcance: Resolución 637 del 21-12-2017 Política general de seguridad de la información en la Subsecretaría de Agricultura.
3. Objetivo General: Verificar los controles y el cumplimiento de la normativa, respecto de lo instruido por la presidencia en el Gab. Pres. N° 001 del 27/04/2017, sobre seguridad de la información, así como los establecido en la política interna en la materia de la Subsecretaría de Agricultura.

II. RESUMEN RESULTADO AUDITORIA

Hallazgos Criticidad Alta	Hallazgos Criticidad Media	Hallazgos Criticidad Baja	Total
0	10	0	10

III. TEMAS RELEVANTES

N°	TEMA
	Punto Crítico 1: Seguridad de los activos informáticos y tecnológicos.
1	Se cuenta con el Procedimiento TI-PRO-10 Control de Inventario de Activos, en el que se señala, por una parte, que el ámbito son todos los activos de información, y por otra, indica que aplica para los procesos IFC, Red Agroclimática y Transferencias, dejando fuera los procesos administrativos y de soporte.
2	Existen dos sistemas de control de bienes tecnológicos. Uno está a cargo de T.I. y el otro de Administración, los cuales no están conciliados entre sí, observándose inconsistencia entre el total de bienes tecnológicos informados en la aplicación de control de activos, los que suman 868, mientras que el total del registro de inventario es 1.242 bienes.
3	De los bienes tecnológicos registrados en el Inventario, considerados en la revisión, 134 equivalente a un 25%, no fueron informados por las unidades, lo que podría indicar que no se encuentran físicamente en esas dependencias y no habrían sido dados de baja en los registros.
4	En el sistema de inventario de la Subsecretaria, 104 bienes (19%), se encuentra registrado en una ubicación o área distinta a lo informado por los responsables de los bienes físicos. Asimismo, 42 activos que se encuentran físicamente en funcionamiento, equivalente a un 8% no están registrados en el inventario.

N°	TEMA
	Punto crítico 2: Uso y acceso a bienes informáticos y Planes de Contingencia para la continuidad de las operaciones.
5	Se observa que en el procedimiento TI-PRO-07 Continuidad del Servicio, los riesgos de mayor impacto, que afectan a los sitios web y sistemas informáticos institucionales, no señalan medidas técnicas para mitigar su acción, estableciendo que la operación de contingencia es: "estar a la espera hasta que el sistema vuelva a estar disponible".
6	De acuerdo con lo señalado en el procedimiento de continuidad, la operación de contingencia considera la provisión para los usuarios internos, una fuente de energía ininterrumpida UPS de respaldo en caso de corte, sin embargo, en la realidad existen procesos críticos de la Subsecretaría como por ejemplo Finanzas y Contabilidad, que no cuenta con este dispositivo.
	Punto Crítico 3: Uso de los servicios de correo electrónico. Seguridad, monitoreo y operatividad eficiente.
7	Se verifican medidas como barreras para el acceso de correos maliciosos y carpetas diferenciadas para mensajes de alta y baja importancia, sin embargo, no hay un procedimiento relacionado con la eliminación o almacenamiento de mensajes, así como los medios y plazos para optar a su respaldo.
	Punto Crítico 4: Acceso a los sistemas de información institucionales y perfiles de usuarios.
8	Se verifica que en el procedimiento TI-PRO-06 Control de Acceso a Sistemas, al igual que otros procedimientos, solo aplica para tres procesos críticos, los que a su vez son los que están considerados en el mapa de riesgos institucional de seguridad de la información, dejando fuera los sistemas financieros y de recursos humanos, entre otros.
	Punto Crítico 5: Uso de redes y servicios de red actualizados según normas de ciberseguridad.
9	De acuerdo con lo instruido por la Presidencia, en Gab. 008 del año 2018, relativo a la protección preventiva de la infraestructura tecnológica y sus datos, se observa que no hay un procedimiento regular para la mantención periódica de estos bienes, que sea conocido por los usuarios, así como su programación, de manera de verificar el estado de los equipos y prevenir su paralización y posible pérdida de información.
10	En cuanto al Gab. 001 del año 2017, que establece como objetivo desarrollar una cultura de ciberseguridad en torno a la educación, se observa que a nivel institucional no se ha definido un Plan de difusión para esta materia, particularmente toda vez que se crean o se realizan modificaciones a los procedimientos de seguridad de la información o activos tecnológicos, de manera que tomen conocimiento de esto todos los usuarios de la Subsecretaría.

IV. OPINIÓN DEL AUDITOR.

Sistema de Control Interno que Requiere Mejoras

V. CONCLUSIONES

Con respecto al objetivo de esta auditoría, es decir, verificar los controles y el cumplimiento de la normativa, respecto de la seguridad de la información, así como los establecido en la política interna en la materia de la Subsecretaría de Agricultura, se concluye que se cumplen razonablemente las disposiciones establecidas en las instrucciones de la presidencia e hitos del programa de mejoramiento de la gestión.

No obstante, se requieren mejoras en lo referido al control y registro de los bienes tecnológicos, según se recomienda en este informe.

Cabe señalar que se establecieron compromisos a través de los cuales se espera subsanar las causas de las observaciones y mejorar las tecnologías de información y comunicaciones TIC, en su conjunto a nivel institucional.

VI. EQUIPO DE TRABAJO

María Luisa Torres T.	Verónica Silva A.
Auditora	Jefa Unidad Auditoría
Ejecución e Informe Final	Planificación y Supervisión
28-11-2018	28-11-2018

SUBSECRETARIA Jefe Unidad Auditoría REVISADO Y FIRMADO