FICHA DE COMPROMISOS DE AUDITORIA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES – TIC	Número ID	ASEG-07
	Fecha	22-11-2018

	HALLAZGO	RECOMENDACIÓN DE AUDITORÍA	COMPROMISO ASOCIADO AL HALLAZGO	FECHA IMPLEMENTACIÓN	MEDIO DE VERIFICACIÓN	CARGO RESPONSABLE IMPLEMENTACIÓN
	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.	Se sugiere hacer extensiva la aplicación del procedimiento de control de activos tecnológicos a todos los bienes informáticos y tecnológicos de la Subsecretaría, incluyendo los procesos administrativos y de soporte.	Dado que el procedimiento TI-PRO-10 Control de Inventario de Activos está asociado con un control de PMG de SSI, se evaluará el impacto de incluir todos los procesos de la Subsecretaría en él, y de ser pertinente, se dejará explícitamente en el procedimiento. IMPLEMENTADA	30/06/2019	TI-PRO-10 Control de Inventario de Activos,	Jefe Departamento TI
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.	Se recomienda revisar y conciliar los bienes del sistema de control de activos tecnológicos con la base de administración.	Se conciliarán los bienes tecnológicos del sistema informático utilizado por T.I. a través de su servicio de Mesa de Ayuda externalizada, con los registrados en el Inventario de Administración. IMPLEMENTADA	30/06/2019	- Sistema Informático - Inventario de bienes tecnológicos.	Jefe Departamento TI

FICHA DE COMPROMISOS DE AUDITORIA

	HALLAZGO	RECOMENDACIÓN DE AUDITORÍA	COMPROMISO ASOCIADO AL HALLAZGO	FECHA IMPLEMENTACIÓN	MEDIO DE VERIFICACIÓN	CARGO RESPONSABLE IMPLEMENTACIÓN
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.	Se debe revisar y conciliar los bienes del sistema de control de activos tecnológicos con los del Inventario y los que se encuentran físicamente en las distintas unidades de la Subsecretaría.	Se conciliarán los bienes tecnológicos del sistema informático con los registrados en el Inventario y los que se ubican físicamente en las distintas áreas de la Subsecretaría. Para el caso de regiones, y si el presupuesto lo permite, se planificará una visita para conciliar el total del inventario.	30/06/2019	Sistema Informático Inventario de bienes tecnológicos Levantamiento físico de los bienes tecnológicos.	Jefe Departamento TI
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.	Se debe revisar y conciliar los bienes del sistema de control de activos tecnológicos con los del Inventario y los que se encuentran físicamente en las distintas unidades de la Subsecretaría.	Se conciliarán los bienes tecnológicos del sistema informático con los registrados en el Inventario y los informados que se ubican físicamente en las distintas áreas de la Subsecretaría. Se debe considerar que los movimientos de equipamiento computacional se informan una vez por cada mes, al final de este, para que sea actualizada su ubicación y registro de movimiento en el sistema de inventario.	30/06/2019	Sistema Informático Inventario de bienes tecnológicos Levantamiento físico de los bienes tecnológicos.	Jefe Departamento TI

IMPLEMENTADA

IMPLEMENTADA

	HALLAZGO	RECOMENDACIÓN DE AUDITORÍA	COMPROMISO ASOCIADO AL HALLAZGO	FECHA IMPLEMENTACIÓN	MEDIO DE VERIFICACIÓN	CARGO RESPONSABLE IMPLEMENTACIÓN
	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".	Se recomienda redefinir una medida de contingencia concreta y eficiente para el procedimiento TI-PRO-07 Continuidad del Servicio.	Se analizarán nuevas medidas de contingencia para el procedimiento TI-PRO-07 Continuidad del Servicio. IMPLEMENTADA	30/06/2019	Procedimiento TI-PRO-07 Continuidad del Servicio.	Jefe Departamento TI
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.	Se recomienda evaluar la factibilidad de provisión de una fuente de energía ininterrumpida UPS de respaldo en caso de corte, para los procesos críticos de la Subsecretaría.	Se analizará la factibilidad de provisión de una fuente de energía ininterrumpida UPS, para los procesos críticos de la Subsecretaría o la reubicación de otras en uso, siempre y cuando los recursos para ello sean asignados. Se presentará documento a DIPRES solicitando presupuesto para la adquisición de UPS.	30/08/2019	Procedimiento TI-PRO-07 Continuidad del Servicio o Documento a DIPRES solicitando presupuesto, según corresponda IMPLEMENTADA	Jefe Departamento TI

	HALLAZGO	RECOMENDACIÓN DE AUDITORÍA	COMPROMISO ASOCIADO AL HALLAZGO	FECHA IMPLEMENTACIÓN	MEDIO DE VERIFICACIÓN	CARGO RESPONSABLE IMPLEMENTACIÓN
	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.	Se sugiere definir y difundir un procedimiento para la eliminación o respaldo de mensajes de correo electrónico que se encuentran almacenados ya sea por larga data o que ocupan mucho espacio.	Actualmente se cuenta con niveles de respaldo que nos permiten resguardar la información contenida en correos electrónicos o carpetas compartidas, adicionalmente se está efectuando una instalación masiva de sistemas de protección para usuarios. De igual forma, se compromete la elaboración de un plan de difusión con información relacionada a este punto.	30/06/2019	Difusión con información relacionada con las buenas prácticas en el uso de correo electrónico.	Jefe Departamento TI

IMPLEMENTADA

	HALLAZGO	RECOMENDACIÓN DE AUDITORIA	COMPROMISO ASOCIADO AL HALLAZGO	FECHA IMPLEMENTACIÓN	MEDIO DE VERIFICACIÓN	CARGO RESPONSABLE IMPLEMENTACIÓN
	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 el sistema de recursos humanos.	Se sugiere hacer extensiva la aplicación del procedimiento de control de acceso a sistemas, para todos los procesos de la Subsecretaría.	Se dejará explícito en el procedimiento TI-PRO-06 Control de Acceso a Sistemas, que aplica para todos los procesos de la Subsecretaría. IMPLEMENTADA	30/06/2019	TI-PRO-06 Control de Acceso a Sistemas	Jefe Departamento TI
	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	Se sugiere establecer un procedimiento para la mantención periódica de los bienes informáticos y tecnológicos, que sea conocido por los usuarios, así como las fechas que les corresponde la revisión de sus equipos.	Se evaluarán las medidas de mantención de los bienes informáticos y tecnológicos a través de un plan anual de mantenimiento preventivo y/o correctivo, los que serán oportunamente comunicados a los usuarios, previa autorización y aprobación de la autoridad respectiva.	30/06/2019	Plan anual de mantenimiento preventivo y/o correctivo para la Subsecretaría. IMPLEMENTADA	Jefe Departamento TI

FICHA DE COMPROMISOS DE AUDITORIA

	HALLAZGO	RECOMENDACIÓN DE AUDITORÍA	COMPROMISO ASOCIADO AL HALLAZGO	FECHA IMPLEMENTACIÓN	MEDIO DE VERIFICACIÓN	CARGO RESPONSABLE IMPLEMENTACIÓN
	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.	Definir un Plan de difusión para los temas relevantes e hitos de ciberseguridad de la información que deben tomar conocimiento los usuarios de la Subsecretaría.	Se trabajará en un Plan de Difusión de Ciberseguridad Institucional para todos los funcionarios de la Subsecretaría con los temas relevantes e hitos del plan general en coordinación con el encargado de Ciberseguridad Ministerial.	30/06/2019	Plan de Difusión de Ciberseguridad Institucional.	Jefe Departamento TI

IMPLEMENTADA

María Luisa Torres T.	Verónica Silva A.	Juan Vasquez
Auditora	Jefa Unidad Auditoria	Jefe Departamento TI.
Planificación, Ejecución e Informe Final	Planificación y Supervisión	Responsable del Proceso
28-11-2018	28-11-2018	28-11-2018

SUBSECRETARIA DE AGRICULTURA Jefe Unidad Auditoria

SUBSECRETARIA DE AGRICULTURA JEFE DEPTO TECHOLOGIAS DE LA INFORMACION