

|  |   |   |   |  |            |
|--|---|---|---|--|------------|
| Ministerio   | INTERIOR Y SEGURIDAD PUBLICA  |   |   | Número   | 9          |
| Servicio   | GOBIERNO REGIONAL DE ATACAMA  |   |   | Código   |            |
| Servicio dependiente   |   |   |   | Páginas  |            |
|  |   |   |   | Fecha emisión  | 12.11.2012 |
| <b>Objetivo Gubernamental N°2, 2012 - Evaluación Integral del Sistema de Control Interno Institucional</b> |   |   |   |  |            |
| Alcance  | Considera la evaluación de los sistemas de control actuales en relación a los cinco componentes del Control Interno, de acuerdo al Marco Integrado de Control Interno, esto es Ambiente de Control, Evaluación de Riesgos, Actividades de Control, Información, Comunicación, y Supervisión o Monitoreo, de acuerdo a la Guía Técnica N° 57 de abril de 2012. |   |   |  |            |
| Opinión Macro Criticidad de la Auditoría (GT 25/2012)  | Sistema de Control Interno Requiere Mejoras   |   |   | Cantidad Total de Hallazgos Identificados                        | 15         |
| Región   | Descripción del Hallazgo  | Efectos   | Recomendaciones Auditoría Interna   | Criticidad del Hallazgo Según Clasificación Guía Técnica 25/2012 |            |
| <b>Ambiente de Control</b>   |   |   |   |  |            |
| ATACAMA  | No se evidencia un mecanismo establecido para educar y comunicar regularmente a la Dirección y a los funcionarios la importancia de los controles internos y elevar el nivel de entendimiento de los controles.   | La inexistencia regular de comunicación hacia los funcionarios en relación a la importancia de los controles internos expone al Servicio a un debilitamiento en la cultura organizacional respecto del proceso de gestión de riesgos y la mitigación de los mismos. | La Jefa de División de Administración y Finanzas debe generar una instancia de información y comunicación hacia los funcionarios en todos sus niveles para relevar la importancia de los controles internos en los distintos procesos que tiene el Servicio.  | Criticidad Alta  |            |
| <b>Evaluación de Riesgos</b>   |   |   |   |  |            |
| ATACAMA  | Inexistencia de un Plan Estratégico Institucional.  | La inexistencia de un Plan Estratégico Institucional, implica un desconocimiento de la estrategia general del Servicio, para cumplir su misión y objetivos institucionales.   | La Jefa de División de Planificación y Desarrollo en el ámbito del Proceso de Acreditación debe avanzar hacia una estructura de participación, con las distintas capacidades del Servicio que se han generado, de manera de contar con una plataforma tecnológica que permita el desarrollo de un plan estratégico institucional. | Criticidad Alta  |            |
| ATACAMA  | Inexistencia de procedimientos para anticipar situaciones de cambio que puedan afectar el normal desenvolvimiento de la entidad.  | No contar con acciones preventivas ante una eventualidad que altere el normal funcionamiento del Servicio.  | La Jefa de División de Administración y Finanzas debe instruir al encargado de seguridad de la información, la correcta aplicación del plan de recuperación ante desastres, en el contexto del PMG-SSI.   | Criticidad Alta  |            |
| <b>Actividades de Control</b>  |   |   |   |  |            |
| ATACAMA  | La función de operaciones TI no está separada de los sistemas y programación; la función de administración de la base de datos no está separada de la programación de aplicaciones y de la programación de sistemas.  | Al no existir segregación de actividades incompatibles, la responsabilidad de los funcionarios no queda expresamente delimitada, en las distintas áreas de competencia.   | La Jefa de División de Administración y Finanzas debe instruir la definición de los roles y funciones de cada funcionario de la Unidad de Informática, para poder determinar si existe o no la segregación de funciones.  | Criticidad Alta  |            |
| ATACAMA  | No existe prohibición para que el personal de TI tenga responsabilidades o deberes incompatibles en los departamentos usuarios.   | Al no existir segregación de actividades incompatibles, la responsabilidad de los funcionarios no queda expresamente delimitada, en las distintas áreas de competencia.   | La Jefa de División de Administración y Finanzas, debe analizar aquellas tareas del personal de TI que no tengan relación con las funciones propias del área de informática, a modo de ejemplo: transparencia activa y pago electrónico de remuneraciones.  | Criticidad Alta  |            |
| ATACAMA  | No existen procesos para revisar periódicamente los privilegios del sistema y controles de acceso a las diferentes aplicaciones y bases de datos dentro de la infraestructura de TI, para determinar si los privilegios del sistema y acceso de control son apropiados.   | La inexistencia de procedimientos documentados no facilita las acciones que deben realizarse en las revisiones y las diferentes aplicaciones dentro de la infraestructura de TI.  | La Jefa de División de Administración y Finanzas, debe considerar este hallazgo para documentar el procedimiento y aplicarlo, dando cumplimiento a los requisitos del PMG SSI.  | Criticidad Alta  |            |
| ATACAMA  | La información electrónica crítica no se encuentra guardada fuera de las instalaciones.   | Si no se evalúa la posibilidad de contar con un resguardo externo, independiente de la infraestructura del edificio que actualmente se resguarda la información, se expone la pérdida ésta ante eventualidades catastróficas.                                       | La Jefa de División de Administración y Finanzas, debe considerar este hallazgo para documentar el procedimiento y aplicarlo, dando cumplimiento a los requisitos del PMG SSI.  | Criticidad Alta  |            |
| ATACAMA  | No existen sistemas para monitorear y responder a interrupciones potenciales del negocio debido a incidentes de intrusión maliciosa, así como para actualizar los protocolos de seguridad para prevenirlos.   | La inexistencia de una herramienta informática de monitoreo impide responder a interrupciones potenciales del Servicio y prevenir las acciones de seguridad para prevenirlos.   | La Jefa de División de Administración y Finanzas, debe disponer de una herramienta informática de monitoreo en relación al comportamiento de la red y del funcionamiento de las aplicaciones, entre otros.  | Criticidad Alta  |            |
| ATACAMA  | No son registrados y revisados automáticamente las violaciones de seguridad y otros incidentes.   | La carencia de revisión y registros de incidentes que atenten la seguridad de información se expone el Servicio a potenciales violaciones de información.   | La Jefa de División de Administración y Finanzas, debe considerar este hallazgo en el Plan de Seguridad de la Información y debiera contemplarse la formación del personal técnico para el uso de esta herramienta.   | Criticidad Alta  |            |

| Región                            | Descripción del Hallazgo  | Efectos   | Recomendaciones Auditoría Interna  | Criticidad del Hallazgo Según Clasificación Guía Técnica 25/2012 |
|-----------------------------------|---|---|--|--|
| <b>Información y Comunicación</b> |   |   |  |  |
| ATACAMA                           | No existen políticas apropiadas para desarrollar y modificar los sistemas de información del Servicio (incluyendo cambios y usos de programas de computación y/o archivos de computación)   | La inexistencia de políticas implica el desconocimiento para la aplicación de ellas.  | La Jefa de División de Administración y Finanzas, debe considerar este hallazgo para documentar el procedimiento y aplicarlo, dando cumplimiento a los requisitos del PMG SSI.   | Criticidad Alta  |
| ATACAMA                           | No existen políticas para la supervisión periódica de los controles de la entidad y no se toman acciones apropiadas para mitigar el potencial de nuevos riesgos.  | La inexistencia de políticas implica el desconocimiento para la aplicación de ellas.  | La Jefa de División de Administración y Finanzas, debe considerar este hallazgo para documentar el procedimiento y aplicarlo, dando cumplimiento a los requisitos del PMG SSI.   | Criticidad Alta  |
| ATACAMA                           | No existe participación por parte de la administración en los proyectos de monitoreo de los sistemas de información y de priorización de recursos.  | Al no existir la asignación de responsabilidades en el monitoreo, se desconoce cuáles le corresponden al ejecutivo del negocio y/o jefe del proyecto tecnológico. | La Jefa de División de Administración y Finanzas, deberá determinar y coordinar cuando proceda la asignación de responsabilidad del monitoreo a un ejecutivo de negocio, el cual cumpla un rol diferente al jefe del proyecto tecnológico. | Criticidad Alta  |
| ATACAMA                           | No existe un plan actual de recuperación de desastres para componentes importantes de la infraestructura de TI.   | La carencia de un plan de recuperación de desastre impide conocer las acciones para mitigar los riesgos.  | La Jefa de División de Administración y Finanzas, debe considerar este hallazgo en el Plan de Implementación de Seguridad de la Información.   | Criticidad Alta  |
| ATACAMA                           | No existe un plan de continuidad de negocio que incorpore el plan de recuperación de desastres y las necesidades de los departamentos usuarios para recuperar oportunamente las funciones críticas, los sistemas, procesos e información del negocio. | La carencia de un plan de continuidad de negocio impide conocer las acciones para mitigar los riesgos que presentan los diferentes usuarios.                      | La Jefa de División de Administración y Finanzas, debe considerar este hallazgo en el Plan de Implementación de Seguridad de la Información.   | Criticidad Alta  |
| <b>Monitoreo</b>                  |   |   |  |  |
| ATACAMA                           | Inexistencia de procedimientos donde le permita a las Jefaturas del Servicio, efectuar revisiones periódicas de control interno, para asegurar que los controles definidos por el Servicio se apliquen de la manera adecuada.                         | La carencia de procedimientos de revisiones periódicas, implica una debilidad de control interno y por ende no permite tomar acciones preventivas.                | Los Jefes de División, deben generar algún procedimiento que le permita asegurarse que los controles de los procesos se efectúan de acuerdo a lo definido.   | Criticidad Alta  |

Según mi mejor feal saber y entendimiento, el presente informe contiene la totalidad de las observaciones relevantes identificadas en esta auditoría, que pudieran tener un impacto significativo para esta institución.



YANETT POLANCO VILLARROEL