ACTA 2911

Fecha de sesión: 2019-12-03 (16:30)

ACTA DE SESIÓN EXTRAORDINARIA NÚMERO DOS MIL NOVECIENTOS ONCE (#2911), CELEBRADA POR EL CONSEJO DIRECTIVO EN LA SALA DE SESIONES UBICADA EN EL PIMA, A LAS DIECISEIS HORAS CON TREINTA Y CINCO MINUTOS, DEL MARTES TRES DE DICIEMBRE DEL DOS MIL DIECINUEVE.

Miembros del consejo:

Asisten los Señores(as) Directivos(as): Sra. Jeannette Ruiz Delgado, Sistema Bancario Nacional. Sr. Rogis Bermúdez Cascante, Presidente Ejecutivo del CNP. Sr. Álvaro Jiménez Cruz, Consejo Nacional de Cooperativas. Gerardo Badilla Castillo, Unión Nacional Gobiernos Locales. Sr. Jorge Gutiérrez Quirós, Sector Exportador.

Ausentes con excusa: Sra. Ana Cristina Quirós Soto, Presidente del Consejo Directivo. Sra. Marcela Guerrero Campos, Presidenta Ejecutiva IFAM.

Se encuentran presente: Sra. Gabriela Brenes Mendieta, Gerente General PIMA. Sr. Álvaro Aguilar Sobalbarro, Auditor Interno, Sra. Lilliana Alfaro Castellón, Auditora Líder, Sr. Joel Brenes Rojas, Encargado de Tecnologías de la Información. Sr. Fabián Cordero Navarro y Sr. Diego Sánchez Quirós, representantes del Despacho Carvajal & Colegiados Contadores Públicos Autorizados S.A.

Acta elaborada por: Sra. Lissa Villalobos Gutiérrez.

Orden del día:

- 1 - Comprobación de quórum y aprobación del orden del día.
- 2 - Aprobación de Acta Nº2910 y firmeza a los acuerdos correspondientes.
- 3 - Oficio DCC-TI-PIMA-2019-01 Informe Auditoría Externa de TI. Expone Fabián Cordero Navarro y Diego Sánchez Quirós Despacho Carvajal & Colegiados Contadores Públicos Autorizados S.A.

Definición de acuerdos:

ARTÍCULO 1: Comprobación de quórum y aprobación del orden del día.

Observaciones:

Comprobado el quórum de ley para sesionar válidamente, se da por iniciada la sesión.

En relación con el orden del día, se solicita atender como punto primero el informe de Auditoría Externa y posteriormente dar lectura y aprobación al Acta N°2910.

Acuerdo 3107:

Las señoras y señores Directivos ante la solicitud expuesta por la señora Jeannette Ruíz Delgado, siendo secundada por el señor Gerardo Badilla Castillo, por unanimidad aprueban el orden del día con la siguiente modificación y

Se resuelve:

Atender como punto primero el informe de Auditoría Externa y posteriormente dar lectura y aprobación al Acta N°2910.

Acuerdo firme.

Gerencia. Asesoría Legal. Control Interno. Auditoría Interna.

ARTÍCULO 2: Aprobación de Acta Nº2910 y firmeza a los acuerdos correspondientes.

Observaciones:

Al respecto, doña Jeannette comenta que ante la solicitud de la Gerencia General del PIMA se tomará un acuerdo paralelo al acuerdo N°3100, con el que se aprobó el Convenio de Cooperación Interinstitucional PIMA-CNP para el uso de una parte del terreno del PIMA, para la construcción de las instalaciones del CNP.

Don Rogis comenta que es razonable, si hubiese alguna duda, atenderla y que las mismas sean aclaradas por los departamentos legales de las instituciones, para que indiquen la forma correcta de plantear las observaciones.

Doña Jeannette aclara que estos ajustes serían de forma, ya que el fondo del convenio está claro.

Con estas observaciones se estaría aprobando el acta N°2910 por los señores Directivos. Se toma nota.

Acuerdo 3109:

Atendiendo la solicitud de la Administración y en aras de que el Convenio de Cooperación Interinstitucional entre el PIMA y el CNP sea de total claridad y aceptación para ambas instituciones y en relación al acuerdo N°3100, por unanimidad

Se resuelve:

Autorizar al señor Rogis Bermúdez Cascante y a la señora Gabriela Brenes Mendieta, para que analicen en conjunto con las Direcciones Jurídicas tanto del Consejo Nacional de Producción como del Programa Integral de Mercadeo Agropecuario, las observaciones que hayan derivado del análisis de dicho convenio.

Una vez que se planteen las observaciones y estas sean incorporadas al documento, se solicita remitir la versión final a este Consejo Directivo para su conocimiento, esto debido a que el convenio se mantiene aprobado en los términos planteados en la sesión ordinaria N°2910.

Acuerdo firme.

Cc: Gerencia General, Asesoría Legal. Control Interno. Auditoría Interna. Dirección CENADA. Dirección REFRINA. Dirección Financiera. Dirección de Estudio y Desarrollo de Mercados. Unidad Ejecutora del Proyecto. Planificación.

ARTÍCULO 3: Oficio DCC-TI-PIMA-2019-01 Informe Auditoría Externa de TI. Expone Fabián Cordero Navarro y Diego Sánchez Quirós Despacho Carvajal & Colegiados Contadores Públicos Autorizados S.A.

Observaciones:

Se recibe a los señores Fabián Cordero Navarro y Diego Sánchez Quirós quienes harán la exposición del informe, también ingresan a la sala los señores Álvaro Aguilar, Joel Brenes y la señora Lilliana Alfaro, quienes estarán presentes durante la exposición de este tema.

Don Álvaro Aguilar agradece el espacio brindado e indica que se procederá a presentar el informe realizado al Área de Tecnologías de la Información por los señores del Despacho Carvajal, adiciona que esta auditoría se encuentra en el plan de trabajo de la Auditoría Interna con el fin de dar cumplimiento a la normativa que la Contraloría establece en el seguimiento de recomendaciones, para lo que se vieron en la obligación de realizar el proceso de licitación, mismo que fue adjudicado al Despacho Carvajal, da la palabra a los señores Fabián Cordero y Diego Sánchez.

Inician la presentación comentando que en la agenda se programó exponer los objetivos generales y específicos, el periodo en el cual realizaron la auditoría, el alcance, los hallazgos, mismos que por ser 24 se comentaran los títulos de cada uno y se van a detallar únicamente los que tienen un riesgo alto para la administración, aclara que cualquier consulta existente sobre los hallazgos con riesgo bajo o medio se podrán aclarar cuando se requiera, para finalizar, indica que se también estaría exponiendo el seguimiento a recomendaciones de periodos anteriores.

Indica que los resultados se expusieron a la administración, posteriormente la administración contó con 3 días para hacer su descargo, mismos que fueron analizados y el resultado final es el que se detalla a continuación:

El periodo de estudio comprendió del 09 de setiembre al 25 de octubre del presente año, los objetivos generales del estudio son: evaluar la gestión de la Tecnología de la Información y Comunicación instalada en el PIMA, en relación con el Sistema de Integración Financiera, SIFPIMA, así como el control interno inherente y la seguridad de la Información Institucional y evaluar la implementación y cumplimiento de las recomendaciones emitidas por auditorías externas de sistemas en períodos anteriores.

Expone los objetivos específicos:

I. Efectuar un diagnóstico de alto nivel que permita evaluar la capacidad actual del actual sistema automatizado, denominado Sistema Integrado de Información Financiera del PIMA (SIFPIMA) para satisfacer las necesidades de las áreas operativas, directivas y de apoyo.

II. Analizar la estructura de control interno definida para la gestión de la Tecnología de la Información instalada al nivel de servicio interno y externo.

III. Evaluación de la estructura de control interno definida para la gestión de la Tecnología de la Información y Comunicación, por citar: a) De la organización del área de informática; b) Del análisis, desarrollo e implementación de sistemas; c) De la Operación del sistema; De la entrada de datos, procesamiento de la información y de la emisión de resultados y d) De la seguridad del área de sistemas.

IV. Evaluación de la operación del Sistema Integrado de Información Financiera del PIMA (SIFPIMA).

V. Evaluar el licenciamiento de la infraestructura informática del PIMA.

VI. Evaluar y certificar la implementación de cada recomendación emitida en los informes de estudios de Auditorías de Sistemas, realizados por despachos de auditores externos.

Comenta que para lograr un análisis más efectivo se reunieron con los usuarios de las áreas que manejan el sistema en sus diferentes procesos y realizaron las evaluaciones tomando en cuenta la satisfacción de los usuarios, la seguridad, entre otros aspectos.

Referente al alcance del estudio, indica que básicamente se orienta a la planeación y orientación de tecnología de la información, la adquisición e implementación, la prestación de servicios y soporte, la administración de los datos y por último el monitoreo y acercamiento.

Doña Lilliana comenta que se solicitó la colaboración del Despacho para calificar los hallazgos en riesgo bajo, medio y alto, lo que ayudará a la Unidad de Control Interno de la institución en cuanto al seguimiento y en la matriz de riesgos institucionales.

Procede a exponer los hallazgos calificados como de riesgo alto:

Hallazgo 2.1. Ausencia de un Plan Estratégico de Tecnologías de Información (PETI) formalmente establecido en el PIMA, informa que ante la solicitud de un plan estratégico de TI, lo que se entregó fue un documento que se elaboró en el año 2007 y se actualizó en el año 2018, sin embargo, dicho documento no cuenta con las características o requerimientos mínimos de un PETI, ya que no tiene una alineación con la planeación estratégica institucional, tampoco muestra los procesos actuales de TI ni un análisis FODA adecuado.

Agrega que las recomendaciones que se hacen son de manera integral y que en este sentido se involucra al Área de Planificación institucional, que debe involucrarse en este proceso para ligar los objetivos y estrategias de TI con los del PIMA y mantenerlos alineados con una revisión constante año a año. Y por parte de TI se deberá dar un seguimiento para asegurar su cumplimiento.

El segundo hallazgo se refiere a las deficiencias en la Planificación Anual Operativa de Tecnologías de Información, refiriéndose a un módulo de planificación en el SIFPIMA, explica que este módulo prácticamente sirve para darle seguimiento al presupuesto, pero no está asociado con la estrategia a nivel institucional. Indica que es importante primero establecer el PETI para luego elaborar la planeación operativa anual en materia de información y que se ejecute de manera ordenada para la consecución de los objetivos institucionales, las recomendaciones van en el sentido de elaborar un PAO que detalle las actividades, planificar los proyectos de TI previa revisión de la Comisión de TI, alinear el plan presupuestario y el plan de infraestructura de TI con el PAO y desarrollar indicadores cualitativos y cuantitativos.

Otro hallazgo se refiere a las deficiencias en la Gestión de Riesgos de Tecnologías de Información, ya que solamente se establece un hallazgo en materia de TI enfocado en el fallo de los sistemas de información, que por su definición no es un riesgo como tal, sino una consecuencia de un riesgo, mismos que se irán viendo en este informe y que no han sido gestionados por el área de TI, la recomendación es que TI realice el proceso de identificación de riesgos para cada uno de los procesos de esta área, para que los mismos sean identificados y comparados en el tiempo y saber si las acciones o mitigadores de cada riesgo están siendo efectivos o no.

Con riesgo bajo menciona la ausencia de una metodología para la gestión de la calidad de los servicios de TI, indica que los servicios de TI tienen que darse en base a un catálogo de servicios que sirve como base para establecer una mejora continua.

Como segundo alcance, referente a la adquisición e implementación, presenta el riesgo que indica deficiencias en los contratos con terceros que brindan servicios relacionados con el SIFPIMA, menciona que todos los relacionados se calificaron como riesgo medio, sin embargo no quiere decir que tengan menor importancia y es necesario atenderlos para que no se lleguen a convertir en riesgos altos, indica que el SIFPIMA terceriza casi la totalidad de sus servicios y no hay un adecuado control de los contratos.

Don Álvaro Jiménez consulta si estas deficiencias en los contratos de dan desde la parte contractual? Le responden que se dan en dos áreas, primero, en el informe se exponen cuales contratos se evaluaron y se indica que hay una serie de oportunidades de mejora, una de esas son los

niveles de servicios que son los indicadores que debe cumplir el proveedor para brindar un adecuado servicio, muchos de los contratos carecen de esta información, por lo que no se puede medir adecuadamente al proveedor. También se encuentra el monitoreo formal que corresponde a TI para minimizar los riesgos y verificar que el proveedor está haciendo un trabajo adecuado.

Otro hallazgo, calificado en riesgo medio es la ausencia de una metodología para el desarrollo e implementación de software en el PIMA, explica que conlleva un riesgo medio ya que va a quedar a criterio de la empresa proveedora, según la metodología que se vaya a implementar, por lo que no se puede estandarizar.

Continúa con la ausencia de un plan de adquisición para tecnología de información en el PIMA, también riesgo medio que debe estar ligado con la parte estratégica y presupuestaria. El siguiente hallazgo indica que no se evidenció la existencia de un procedimiento para el mantenimiento de la infraestructura tecnológica del PIMA, si bien se da un mantenimiento preventivo y correctivo existe un programa de trabajo que establece la periodicidad, los resultados, informes y demás, informa que en el PIMA no existe.

El siguiente hallazgo menciona debilidades en el proceso de gestión de cambios en los sistemas de información del PIMA, entiéndase los cambios a la infraestructura general, impresoras, bases de datos y demás, se recomienda establecer un procedimiento que acompañe la función del Aranda.

El tercer alcance referido a la prestación de servicio y soporte establece varios hallazgos, el primero y segundo con riesgo medio son: la ausencia de controles para el seguimiento formal al cumplimiento de los contratos con terceros que brindan servicios de tecnologías de información, ya que no están establecidos los controles ni cómo se medirá el servicio; y la ausencia de un plan de continuidad de tecnología de información, expone que aunque se da el respaldo de la información con antivirus y otras medidas operativas, no existe un plan como tal que garantice al PIMA cuáles serán los procesos críticos.

Continúa con dos riesgos bajos: la ausencia de un procedimiento para la administración de la configuración de Tecnologías de Información, ya que no existe una línea base que permita transparencia sin afectar el servicio; y que no se evidenció la existencia de las capacitaciones impartidas a los funcionarios del PIMA referente al uso del SIFPIMA, no existe un programa de capacitación formal.

El siguiente hallazgo tiene un riesgo medio, se refiere a las deficiencias en la seguridad física del cuarto de servidores del PIMA, menciona que si bien es cierto que existe un proyecto para tener las bases de datos críticas en la nube, durante la auditoría se conoció que esas bases de datos se mantienen en las instalaciones del PIMA, mismas que son deficientes en cuanto a estructura física y presentan un riesgo para el almacenamiento de datos.

Continúa con el cuarto alcance, que menciona la administración de los datos, presenta 6 hallazgos que se clasificaron con riesgo bajo y medio: la ausencia de un procedimiento para la gestión de la capacidad y disponibilidad de la plataforma tecnológica y de un modelo de monitoreo de la infraestructura de TI, la ausencia de un procedimiento para la gestión de respaldos de información, ya que si bien se realizan respaldos, al solicitar la información no se evidenció la periodicidad, otro hallazgo es la ausencia de un procedimiento para la gestión de roles y permisos de los usuarios, otro son las eficiencias en la parametrización de la seguridad lógica del sistema SIFPIMA, también la inexistencia de estudios de vulnerabilidad de la red institucional del PIMA y por último, no se evidenció la existencia de una política de seguridad de la información, explica que hay una falta de evidencia respecto a las acciones que se realizan y que no se tiene identificada la información, ni cuáles son los datos más sensibles para establecer categorías y medidas de seguridad institucionales, en este tipo de políticas de seguridad menciona la ISO 27001 que son estándares comprobados en materia de seguridad de la información, que pueden ser de ayuda para la administración al momento de establecer las políticas de seguridad de la información.

Continúa con el hallazgo referido a la dependencia hacia proveedores de servicios para el mantenimiento de la plataforma tecnológica, explica que se determinó que el PIMA cuenta con contratos de servicios, tanto para el mantenimiento de la plataforma tecnológica, como para el mantenimiento del SIFPIMA, el encargado de TI delega ciertas responsabilidades importantes a los proveedores, como la administración local de la plataforma, dando un control total al proveedor respecto a datos y plataforma tecnológica, además el proveedor es el encargado de administrar los respaldos y gestiona la información desde sus instalaciones, de manera externa, y se encargan de desarrollar y realizar los pases de producción, esto debido a que el área de TI no está en capacidad de dar mantenimiento en su propio sistema, ante algún cambio es el proveedor es el que debe realizar dicho cambio, con el riesgo de que al ser una plataforma obsoleta no cualquier proveedor tiene el conocimiento para trabajar en ella, por lo que se depende de un único proveedor.

Ante lo expuesto, recomiendan establecer un plan de contingencia que abarque los procesos y el SIFPIMA como tal, además mantener el mantenimiento de la plataforma tecnológica a lo interno de TI y gestionar el ciclo de vida de los activos de TI para no llegar a la obsolescencia de las herramientas.

El siguiente hallazgo muestra deficiencias en la automatización de procesos, funcionalidad e integraciones en el sistema SIFPIMA, comenta que se reunieron con los usuarios para verificar la funcionalidad del sistema y se detectaron varias deficiencias en cuanto a la automatización de los procesos del sistema, señala que revisaron los módulos de proveeduría, recursos humanos, servicios generales, financiero, tesorería, contabilidad, casetas, red de frío y CENADA, a manera de resumen expone que sobre la automatización de procesos en el módulo de Contabilidad, se debe anular y volver a revisar los asientos para los pagos mediante datafono para las mensualidad en la Red de Frío, ya que los asientos originales no registran los montos de comisión ni el IVA, se debe de generar el reporte de activos por clasificación y se debe manipular en el área de contabilidad para hacer la categorización adecuada en el catálogo de cuentas, algunas de las cuentas no se encuentran en el nivel 8 como es requerido por lo que se deben completar de forma manual. Igual sucede con las acciones de personal en el módulo de Recursos Humanos y para el módulo de REFRINA, cuando se realiza el pago con tarjetas se llevan algunos registros de forma manual. Agrega que se verificó que existen varios Arandas que aún no se han atendido y sobre la conexión al sistema, indica que los enlaces son lentos y en algunos casos se muestran mensajes de error que no permiten el trabajo fluido.

Por lo anterior, se recomienda realizar un estudio para determinar la viabilidad de actualizar la plataforma SIFÏMA y establecer fechas para atender cada hallazgo y que los usuarios del sistema utilicen la plataforma ARANDA para solicitar los ajustes que se requieran.

Continúa con el alcance de monitoreo y aseguramiento, el primer hallazgo, clasificado como riesgo bajo indica que hay ausencia de evaluaciones de control interno de los procesos de gestión del Área de TI, comenta que actualmente el Área de Control Interno sí realiza un seguimiento al cumplimiento de las recomendaciones de las auditorías y realiza una verificación del SEVRI y del IGI, pero no existe un procedimiento como tal.

El último hallazgo es el no cumplimiento de recomendaciones emitidas en estudios de auditoría tanto interna como externa de TI, datos que se van a mostrar en la segunda parte del estudio.

Don Rogis consulta si se basaron en alguna norma para realizar el informe expuesto? Se le contesta por parte de don Fabián que específicamente se basan en la metodología del despacho, por conocimiento y que no utilizan una norma como tal. Don Rogis comenta algunos ejemplos sobre diferentes normas que se aplican según los temas a auditar, destaca que para medir riesgo se usa la 31000, y así menciona una cantidad de normas que se utilizan, da como ejemplo un hallazgo que indica la ausencia de un procedimiento, mismo que se clasificó con riesgo bajo, más adelante se indica la ausencia de otro procedimiento, clasificado como riesgo medio, lo que le genera una confusión en cuanto a criterios y explica que la utilización de las normas es un referente para la medición de los riesgos, en este caso, consulta cómo se midieron? Don Fabián comenta que la categorización del riesgo se da según el impacto, por lo que dependiendo de las áreas podría

desembocar en un riesgo bajo, medio o alto. Básicamente el criterio está basado en la probabilidad y el impacto, que lo determina, la experiencia del auditor y el área que se está evaluando

Don Rogis comenta que le parece importante contar siempre con una matriz que indique la causa raíz, el efecto, el impacto y las formas de contingencia para minimizar dicho impacto.

Don Fabián indica que sí toman en cuenta algunas normas y que el sistema que utilizan ya tiene inmerso en cada uno de los procesos a evaluar el riesgo, lo que se hace es que los Auditores toman ese marco de referencia y lo trasladan a la situación institucional.

Doña Jeannette comenta que el estudio es bastante integral, y que sin entrar en detalles de riesgos bajos, medios o altos, se muestra que se tienen deficiencias marcadas y que en esta época ya deberían de haberse resuelto, empezando por el tema de planificación cuando se habla de tener una estrategia de tecnología alineada con la actividad productiva que se está dando en la institución, y al no tener una estrategia es difícil realizar una evaluación real de los avances que se han obtenido. Lo que lleva a problemas subsecuentes muy amplios, por ejemplo, la gestión de riesgos tecnológicos en una época donde la ciberseguridad es uno de los temas más importantes que se dan y no puede ser que se tenga una plataforma vulnerable.

Agrega que el tema de depender de proveedores es caro y es un riesgo muy alto por tener que depender del tiempo de respuesta y se puede materializar una pérdida de información o de otro tipo que tenga un impacto importante para la institución. Igualmente al no contar con un centro alterno de datos se presenta una vulnerabilidad grave, por lo que se debe trabajar. Igualmente considera que el contacto con políticas es primordial, ya que cuando se ahonda en la operativa real de tecnología, el hecho de no haber invertido durante algunos años para renovar el equipo de soporte, podría causar un problema serio que se puede convertir en un costo alto si la información se pierde. Considera que este informe debería permitir solicitar la elaboración de una estrategia, contar con un plan de acción que tiene que ser a corto, mediano y largo plazo, sabiendo que se tiene una limitante en el recurso humano y que existen temas que son muy delicados. Luego de estas acciones se deberán implementar políticas de seguridad de la información y medir los riesgos e impactos reales y a partir de ahí buscar los mecanismos idóneos.

Se da la palabra a Joel Brenes, quien indica que el hecho de que no exista la documentación actualizada de los procedimientos, no quiere decir que las medidas y contingencias no se hayan tomado, explica que en el PIMA se cuentan con muy buenas medidas de control y medición que permiten llevar un control en cada uno de los sistemas, no obstante, en materia de recursos recalca que sí se requieren recursos, principalmente recurso humano ya que hasta hace cuatro meses él era quien se encargaba de TI, por casi 18 años se ha hecho cargo del departamento, agrega que él no puede descuidar la operación por la documentación, por lo que solicita tener presente todos estos datos, sin embargo, comenta que conversando son los señores auditores, expresó que esto es una radiografía de lo que se tiene, que no se puede ocultar y que requiere un apoyo de la Gerencia y de una Comisión de Informática, para poder implementar varias cosas que no se han podido.

Doña Jeannette indica que por esta razón el plan de acción va a ser fundamental, ya que va a establecer tiempos de respuesta, presupuestos, responsables y demás y si es necesario más recurso humano se debe contemplar en el plan de acción, a sabiendas de que una sola persona no da abasto con esta tarea, y se deben apoyar las decisiones que se tomen.

Don Joel agrega que se suma la incorporación del Mercado Chorotega que ha requerido atención y ha desgastado en el sentido de que es otro mercado que requiere toda la atención.

Se solicita a don Fabián continuar con la segunda parte del informe.

Inicia exponiendo el segundo objetivo: Evaluar la implementación y cumplimiento de las recomendaciones emitidas por auditorías externas de sistemas en períodos anteriores. Menciona que existen auditorías del año 2008 y se dio seguimiento a cada recomendación, a manera de resumen expone algunos gráficos.

La primeras son las recomendaciones dirigidas a áreas usuarias, realizada por la auditoría interna del PIMA, de las 10 recomendaciones que surgieron en su momento se encontraron 2 corregidas, 5 en proceso, 3 pendientes, lo que porcentualmente significa un 50% en proceso, 20% corregidas y 30% pendientes de implementarse. Dentro de los hallazgos de este informe estaba la falta de planificación, el PETI desalineado, recargo de trabajo en TI, falta de control en los contratos, infraestructura física en condiciones no adecuadas.

Otra de las auditorías realizadas por auditoría interna, dirigida a TI, da como resultados 2 hallazgos en proceso, 2 pendientes y uno corregido, para un total de 40% pendientes, 40% en proceso y 20% corregidos. Dentro de las recomendaciones están que no se han establecido responsabilidades por errores pasados y evaluar la viabilidad, planificar y coordinar con la Ingeniera Civil de la Institución el rediseño y las mejoras a la infraestructura del lugar donde albergan los servidores del PIMA.

Don Álvaro Jiménez consulta que cuando se indica que no se han establecido responsabilidades por errores pasados, de qué se trata? Don Fabián responde que en ese informe se indicó que no se establecieron responsables para atender las recomendaciones dadas en ese momento, con tiempo, indicadores y recursos.

Doña Lilliana agrega que cuando se emitieron las recomendaciones, en aquel momento no era la práctica establecer un plan de acción que instituyera una persona responsable de cada acción, por lo que se encuentra pendiente.

Don Fabián continúa con el siguiente reporte referente a auditorías externas realizadas por otras firmas, existe un estudio del año 2008 realizado por la firma Deloitte, en la cual se dieron 47 hallazgos de los cuales 5 están corregidos, 17 están en proceso y 25 pendientes, lo que porcentualmente se registra como 53% pendientes, 11% corregidas y 36% en proceso de implementación, recalca que han tenido 11 años en los que la administración no ha podido atender estos hallazgos.

Los hallazgos en esta oportunidad se referían a la definición de la Unidad de Informática, documentación y comunicación de políticas y procedimientos, modelo de riesgo de tecnología (evaluación de riesgos) y estructura de control interno, ausencia de portafolio de proyectos, ausencia de un plan estratégico formal de tecnología de la información. Además, no se disponen de controles para los niveles de servicio con proveedores externos y usuarios internos, deficiencias en la administración de pases al ambiente de producción, la administración de la seguridad de los sistemas, servidores y bases de datos no está centralizada y los respaldos de información no se resguardan en medios externos. Menciona que el detalle de cada uno de estos hallazgos se encuentra en el informe.

Pasando a otro estudio de auditorías externas, en el 2010 se dio un hallazgo que indicó que existen inconsistencias en la información de la base de datos del SIFPIMA, indica que en solo este hallazgo se dieron 154 recomendaciones y se verificó el estado de estas, dando como resultado, solamente 5 aspectos se corrigieron.

El siguiente estudio se realizó en el año 2009, de los 23 hallazgos, 6 fueron corregidos, 6 en proceso, 10 están pendientes y 1 no aplica, porcentualmente 44% pendientes, 26% en proceso, 26% corregidas y el restante 4% corresponde al hallazgo que no aplica. Dentro de las recomendaciones emitidas en este informe, se detalla la inconsistencia en la información de la base de datos del SIFPIMA, carencia de análisis de vulnerabilidades a la red de la institución, dependencia de los servicios con terceros, switches, terminales remotas (VTYS) sin restricciones de acceso y la puerta de cuarto de servidores.

El resumen general de este informe, mismo que actualizó la situación del PIMA en materia de TI, expone que existen recomendaciones emitidas hace 11 años y que si bien es cierto las recomendaciones no son las mismas todos los años, el fondo sí se mantiene, por ejemplo el tema del PETI, bases de datos, PAO, riesgos y otros, esto para un total, sin contar el informe de este periodo, de 86 hallazgos en donde 14 están corregidos, 31 en proceso, 40 pendientes y 1 no aplica, lo que da

un 36% de recomendaciones en proceso, el 47% está pendiente, el 16% corregido y un 1% no aplica, si se agrega.

En el resumen de cantidad de recomendaciones sí se contemplaron las 24 recomendaciones emitidas en el presente informe, para un total de 110 hallazgos con 228 recomendaciones pendientes de atender desde el año 2008 a la fecha.

Al no haber más comentarios ni preguntas, doña Jeannette concluye indicando que lo que procede es la solicitud del plan de acción con detalle de responsables y tiempos, ya que esto deteriora el record que lleva la administración de ir resolviendo temas pendientes, muchos son temas antiguos que posiblemente se puedan conjugar en algunos temas, siendo esto parte del análisis que debe hacer la administración.

Don Álvaro Jiménez indica que es importante prestar atención y tomar las precauciones del caso, ya que muchos de los hallazgos están catalogados como riesgo alto y eso preocupa, por eso la importancia del plan, comenta que particularmente anotó el tema de la dependencia de proveedores, así como la escasez del recurso humano, ya que es importante y entendible, sin embargo la administración tiene una gran tarea de la cual debe ocuparse.

Don Rogis comenta que a veces cuando son temas de auditoría y temas de impacto se debe ser lo más claro posible, indica que si fuera él quien debe recibir estas recomendaciones, posiblemente indicaría que no cuenta con la información suficiente, da como ejemplo un hallazgo que indica documentación y comunicación de políticas y procedimientos, pero considera que falta información, don Fabián le responde que para cada hallazgo existe un informe detallado.

Doña Lilliana agrega que esos informes son los que se realizaron en años anteriores por otras firmas consultoras y que cada informe tiene su detalle, agrega que esos hallazgos son de conocimiento del funcionario del TI y fueron aceptados en su momento y discutidos con la Gerencia en su momento y lo que se hizo fue un resumen como referencia. Agrega que el mismo funcionario del 2008 es el que está en este momento, por lo que conoce cada tema.

Don Fabián concluye explicando que incluso para ellos como auditores a veces es difícil entender qué quiso decir una persona hace 11 años, por eso solamente se mencionaron.

Don Álvaro Aguilar comenta que dentro de la metodología empleada, el despacho hizo 2 avances de su informe y una vez que estuvo finalizado, se procedió a comentarlo con la administración en presencia del encargado de TI, mismo que estaba en la institución desde el año 2008, para conocer si tenían algún elemento para refutar alguna de las recomendaciones, se dio el plazo y la administración no aportó nada, por lo que se mantuvo el informe que se discutió entre la Administración, la Auditoría Interna y la Auditoría Externa.

Don Joel comenta que hay muchos elementos de las auditorías externas anteriores que prácticamente ellos había puesto al 100%, inclusive en un reporte anterior, se había dado casi por completo, pero el plazo de 3 días para recopilar toda la información y volverlas a mostrar era muy difícil y no pudo hacerlos, máxime que se está en un periodo de transición de un proyecto que están desarrollando, por lo que se tornó difícil brindar toda la evidencia, sin embargo, indica que hay muchas acciones que ya fueron desarrolladas.

Se agradece a los señores que estuvieron presentes en este punto y se retiran de la sala.

Se consulta sobre el desempeño del encargado de TI y doña Gabriela responde que es el funcionario que siempre ha estado en el puesto, siendo un departamento unipersonal y con mucha carga de trabajo, la administración espera buscar la forma para ahondar todo lo que se encuentra pendiente.

Acuerdo 3108:

Luego de conocer el oficio DCC-TI-PIMA-2019-001 y el informe correspondiente a la Auditoría de Sistemas de Información, emitidos por el Despacho Carvajal & Colegiados Contadores Públicos

Autorizados S.A. y de escuchar la exposición brindada por los señores Fabián Cordero Navarro y Diego Sánchez Quirós, por unanimidad

Se resuelve:

Dar por conocido el informe de Auditoría de TIC, SIFPIMA y Seguimiento de Recomendaciones - Auditoría de Sistemas de Información, e instruir a la administración para que formule una propuesta de plan de acción para la atención de los hallazgos expuestos en el informe antes mencionado, dicho plan debe incluir tiempos de respuesta, responsables, presupuesto y demás detalles, de tal forma que se pueda atender en tiempo y forma todos los hallazgos que datan del 2008, se solicita presentar el plan ante este Consejo Directivo en un plazo razonable, mismo que no debe exceder los tres meses.

Además se considera que se debe trabajar en forma paralela en el diseño de una estrategia de tecnología que contemple los temas que se exponen en los hallazgos, lo anterior para poder alinear el servicio que TI brinda a la actividad productiva del PIMA.

Acuerdo firme.

Cc: Gerencia General, Asesoría Legal. Control Interno. Auditoría Interna. Dirección CENADA. Dirección REFRINA. Dirección Financiera. Dirección de Estudio y Desarrollo de Mercados. Unidad Ejecutora del Proyecto. Planificación. Tecnología de la Información.

Se levanta la sesión extraordinaria número dos mil novecientos once, a las dieciocho horas con siete minutos del martes tres de diciembre del dos mil diecinueve.

Jeannette Ruíz Delgado — Presidente Consejo Directivo Ad Hoc

Gerardo Badilla Castillo — Secretario Consejo Directivo Ad Hoc