DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
UNIDAD DE AUDITORÍA DE SISTEMAS

INFORME FINAL

Comisión Nacional de Riego

Número de Informe: 305/2016
3 de agosto de 2016

CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
UNIDAD DE AUDITORÍA DE SISTEMAS

PMET. N° 13.701/2016
DAA. N° 1.887/2016
REF. N° 195.623/2016

REMITE INFORME FINAL QUE INDICA.

SANTIAGO, 03.AGO16 *057039

Cumplo con enviar a Ud., para su conocimiento y fines pertinentes, el Informe Final N° 305, de 2016, debidamente aprobado, sobre auditoría al macroproceso de tecnologías de la información, practicada en la Comisión Nacional de Riego.

Saluda atentamente a Ud.,

JORGE BERMÚDEZ SOTO
Contralor General de la República

13:12 05.08.2016 OF PARTES MINAGRI

AL SEÑOR
CARLOS FURCHE GUAJARDO
MINISTRO DE AGRICULTURA
PRESENTE

RTE
ANTECED

CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
UNIDAD DE AUDITORÍA DE SISTEMAS

PMET. N° 13.701/2016
DAA. N° 1.888/2016
REF. N° 195.623/2016

REMITE INFORME FINAL QUE INDICA.

SANTIAGO, 03.AGO 16 * 057040

Adjunto, remito a Ud., para su conocimiento y fines pertinentes, Informe Final N° 305, de 2016, debidamente aprobado, sobre auditoría al macroproceso de tecnologías de la información, practicada en la Comisión Nacional de Riego.

Sobre el particular, corresponde que esa autoridad adopte las medidas pertinentes, e implemente las acciones que en cada caso se señalan, tendientes a subsanar las situaciones observadas; aspectos que se verificarán en una próxima visita que practique en esa entidad este Organismo de Control.

COMISION NACIONAL DE RIEGO
05 AGO 2016
OFICINA DE PARTES

Saluda atentamente a Ud.,

POR ORDEN DEL CONTRALOR GENERAL
PRISCILA JARA FUENTES
ABOGADO
Jefe División de Auditoría Administrativa

A LA SEÑORA
SECRETARIA EJECUTIVA
COMISIÓN NACIONAL DE RIEGO
PRESENTE

RTE
ANTECED

CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
UNIDAD DE AUDITORÍA DE SISTEMAS

PMET. N° 13.701/2016
DAA. N° 1.889/2016
REF. N° 195.623/2016

REMITE INFORME FINAL QUE INDICA.

COMISION NACIONAL DE RIEGO
05 AGO 2016
OFICINA DE PARTES

SANTIAGO, 03.AGO 16 * 057041

Cumplo con enviar a Ud., para su conocimiento y fines pertinentes, el Informe Final N° 305, de 2016, debidamente aprobado, sobre auditoría al macroproceso de tecnologías de la información, practicada en la Comisión Nacional de Riego.

Saluda atentamente a Ud.,

POR ORDEN DEL CONTRALOR GENERAL
PRISCILA JARA FUENTES
ABOGADO
Jefe División de Auditoría Administrativa

AL SEÑOR
COORDINADOR DE LA UNIDAD DE AUDITORÍA INTERNA
COMISIÓN NACIONAL DE RIEGO
PRESENTE

RTE
ANTECED

CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
UNIDAD DE AUDITORÍA DE SISTEMAS

PMET. N° 13.701/2016
DAA. N° 1.890/2016
REF. N° 195.623/2016

REMITE INFORME FINAL QUE INDICA.

SANTIAGO, 03.AGO 16 * 057042

Cumplo con enviar a Ud., para su conocimiento y fines pertinentes, el Informe Final N° 305, de 2016, debidamente aprobado, sobre auditoría al macroproceso de tecnologías de la información, practicada en la Comisión Nacional de Riego.

Saluda atentamente a Ud.,

POR ORDEN DEL CONTRALOR GENERAL
PRISCILA JARA FUENTES
ABOGADO
Jefe División de Auditoría Administrativa

Jefe Subrogante
Unidad Técnica de Control Externo

05 AGO. 2016

AL SEÑOR
JEFE DE LA UNIDAD TÉCNICA DE CONTROL EXTERNO (S)
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
CONTRALORÍA GENERAL DE LA REPÚBLICA
PRESENTE

RTE
ANTECED

CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
UNIDAD DE AUDITORÍA DE SISTEMAS

PMET. N° 13.701/2016
DAA. N° 1.891/2016
REF. N° 195.623/2016

REMITE INFORME FINAL QUE INDICA.

SANTIAGO, 03.AGO 16 * 057043

Cumplo con enviar a Ud., para su conocimiento y fines pertinentes, el Informe Final N° 305, de 2016, debidamente aprobado, sobre auditoría al macroproceso de tecnologías de la información, practicada en la Comisión Nacional de Riego.

Saluda atentamente a Ud.,

POR ORDEN DEL CONTRALOR GENERAL
PRISCILA JARA FUENTES
ABOGADO
Jefe División de Auditoria Administrativa

ROSA MORALES CAMPOS
Jefe Unidad de Seguimiento
División de Auditoria Administrativa

05 AGO. 2016

A LA SEÑORA
JEFA DE LA UNIDAD DE SEGUIMIENTO
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
CONTRALORÍA GENERAL DE LA REPÚBLICA
PRESENTE

RTE
ANTECED

CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
UNIDAD DE AUDITORÍA DE SISTEMAS

PMET. N° 13.701/2016
DAA. N° 1.892/2016
REF. N° 195.623/2016

REMITE INFORME FINAL QUE INDICA.

SANTIAGO, 03.AGO16*057044

Cumplo con enviar a Ud., para su conocimiento y fines pertinentes, el Informe Final N° 305, de 2016, debidamente aprobado, sobre auditoría al macroproceso de tecnologías de la información, practicada en la Comisión Nacional de Riego.

Saluda atentamente a Ud.,

RECIBIDO EN UNIDAD DE SUMARIOS
FISCALIA
05 AGO. 2016
CONTRALORIA GENERAL
DE LA REPUBLICA

POR ORDEN DEL CONTRALOR GENERAL
PRISCILA JARA FUENTES
ABOGADO
Jefe División de Auditoría Administrativa

A LA SEÑORA
JEFA DE LA UNIDAD DE SUMARIOS DE FISCALÍA
CONTRALORÍA GENERAL DE LA REPÚBLICA
PRESENTE

RTE
ANTECED

CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
UNIDAD DE AUDITORÍA DE SISTEMAS

PMET. N° 13.701/2016
DAA. N° 1.893/2016
REF. N° 195.623/2016

REMITE INFORME FINAL QUE INDICA.

SANTIAGO, 03. AGO 16 * 057045

Cumplo con enviar a Ud., para su conocimiento y fines pertinentes, el Informe Final N° 305, de 2016, debidamente aprobado, sobre auditoría al macroproceso de tecnologías de la información, practicada en la Comisión Nacional de Riego.

Saluda atentamente a Ud.,

POR ORDEN DEL CONTRALOR GENERAL
PRISCILA JARA FUENTES
ABOGADO
Jefe División de Auditoría Administrativa

OFICINA DE PARTES CONTRALORIA GENERAL DE LA REPÚBLICA
G. SALAZAR E.
Nº 4

AL SEÑOR
MARCELO PARRA VELÁSQUEZ
CALLE TRINIDAD N° 600
COMUNA DE LA FLORIDA
PRESENTE

RTE
ANTECED

CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
UNIDAD DE AUDITORÍA DE SISTEMAS

Resumen Ejecutivo Informe Final N° 305 de 2016

Comisión Nacional de Riego

Objetivo: La fiscalización tiene por finalidad ejecutar una auditoría al Sistema Electrónico Ley 18.450 y a los contratos informáticos de la Comisión Nacional de Riego, CNR, en el período comprendido entre el 1 de enero de 2014 y el 31 de diciembre de 2015.

Preguntas de la Auditoría:

- ¿Se toman medidas ante incumplimientos de las obligaciones estipuladas en las bases de las contrataciones?
- ¿El Sistema Electrónico Ley 18.450 tiene implementados mecanismos de seguridad, integridad y confidencialidad de la información?

Principales Resultados:

- Se advirtió la omisión en la definición de una fecha de vencimiento para hacer exigible el eventual cobro por concepto de garantía por la prestación de las órdenes de compra ID N^{os} 870-117-CM15 y 870-118-CM15; y la inexistencia de documentación para ejecutar el examen de las eventuales multas asociadas a las órdenes de compra ID N^{os} 870-965-CM14 y 870-981-CM14, ante lo cual, en lo sucesivo, la repartición deberá definir e incorporar las fechas asociadas a la provisión de bienes o servicios, en los convenios que establezca con los proveedores, lo que será validado en futuras auditorías.
- La plataforma del Sistema Electrónico Ley 18.450, evidenció la carencia de controles en la asignación de perfiles de acceso, dado que cualquier persona puede acceder y modificar sus privilegios a otros que no han sido autorizados por sistema, logrando inclusive ser administrador de la plataforma. El servicio deberá evaluar y corregir lo advertido, informando su estado de avance en un plazo de 60 días hábiles, contados desde la recepción del presente informe.
- Sobre el mismo sistema, se corroboró que por medio del uso de ataques informáticos orientados a la inyección de código ejecutable en la capa lógica de la aplicación, se accede a toda la información almacenada en la base de datos, quedando expuesta la información confidencial de los concursos y usuarios de la plataforma. La CNR deberá tomar medidas tendientes a solucionar las brechas de seguridad detectadas, a fin de resguardar la confidencialidad de la información, evaluando el estado actual del sistema, informando dentro del plazo citado.
- Para el sistema aludido, en el perfil de consultor, se evidenció que permite el ingreso de comandos no autorizados, posibilitando listar los formularios de costos, superficie y postulación, además permite consultar datos de los postulantes a concursos a través del formulario de búsqueda. La institución deberá levantar un análisis de las causales de la falla de seguridad, junto con informar el estado de avance de las medidas correctivas aplicadas, en el mismo período.

CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
UNIDAD DE AUDITORÍA DE SISTEMAS

PMET N° 13.701/2016

INFORME FINAL N° 305, DE 2016, SOBRE AUDITORÍA DE SISTEMAS, EFECTUADA EN LA COMISIÓN NACIONAL DE RIEGO.

SANTIAGO 03 AGO. 2016

En cumplimiento del plan de fiscalización anual de este Organismo de Control para el año 2016, y en conformidad con lo establecido en la ley N° 10.336, de Organización y Atribuciones de la Contraloría General de la República, y en el artículo 54, del decreto ley N° 1.263, de 1975, Orgánico de Administración Financiera del Estado, se efectuó en la Comisión Nacional de Riego, un examen al macroproceso de Tecnologías de la Información, TI.

La revisión fue ejecutada por el equipo integrado por los señores Rodrigo González Aróstegui, Víctor Garcés Almonacid y Daniel Caviedes González, auditores los dos primeros y supervisor el último.

JUSTIFICACIÓN

En la presente auditoría se tuvo en cuenta la denuncia N° W001133, de 2015, presentada por [redacted]z, ex-funcionario de la Comisión Nacional de Riego, sobre incidencias funcionales y de seguridad de la información en el actual sistema encargado del proceso de entrega de bonos regulados por la ley N° 18.450, que Aprueba Normas para el Fomento de la Inversión Privada en Obras de Riego y Drenaje, el que permitiría, entre otras cosas, el acceso no autorizado a datos sensibles del proceso de postulación, impidiendo proveer de un servicio de calidad, tanto a los usuarios internos de la repartición como externos.

ANTECEDENTES GENERALES

El artículo 1° del decreto con fuerza de ley N° 7 de 1983, del ex Ministerio de Economía, que fija el texto refundido del decreto ley N° 1.172, de 1975, que creó la Comisión Nacional de Riego, define a dicha entidad como una persona jurídica de derecho público, que se relaciona con el Gobierno a través del Ministerio de Agricultura, cuyo objeto es asegurar el incremento y mejoramiento de la superficie regada del país.

AL SEÑOR
JORGE BERMÚDEZ SOTO
CONTRALOR GENERAL DE LA REPÚBLICA
PRESENTE

Contralor General
de la República

En lo que atañe a las principales funciones y atribuciones que le corresponde ejercer a dicho organismo, el artículo 3° del mismo cuerpo legal señala, entre otras, las siguientes:

a) Evaluar los proyectos de riego que elabore o se le presenten.

b) Celebrar convenios con particulares o con empresas nacionales o extranjeras sobre estudios o proyectos integrales de riego.

c) Supervigilar, coordinar y complementar la acción de los diversos organismos públicos y privados que intervienen en la construcción, destinación y explotación de obras de riego.

Cabe anotar que, mediante oficio DAA. N° 1.383, de 11 de mayo de 2016, de este origen, fue puesto en conocimiento de la Secretaria Ejecutivo (S), de manera reservada, el preinforme de observaciones N° 305, de la señalada anualidad, con la finalidad de que formulara los alcances y precisiones que, a su juicio procedieran, lo que se concretó, de manera extemporánea, a través de oficio ORD. N° 1.906, de 2 de junio del referido año, cuyos antecedentes aportados han sido igualmente considerados para la elaboración del presente informe final.

OBJETIVO

La fiscalización tuvo por finalidad ejecutar una auditoría al aplicativo precitado y a contratos informáticos de la Comisión Nacional de Riego, considerando los aspectos administrativos relacionados con las licitaciones, cumplimiento de contrato y técnicos relacionados con políticas, normas, prácticas y procedimientos de control, vinculados con los sistemas basados en las TI, incluidas aquellas actividades de tipo manual o automatizadas que se desarrollan en el entorno de tal aplicativo, para el período comprendido entre el 1 de enero de 2014 y el 31 de diciembre de 2015.

Además, se evaluó el cumplimiento de la normativa relacionada con las TI, de conformidad con lo dispuesto en los decretos N^{os} 83, de 2004, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos; y 181, de 2002, que Aprueba Reglamento de la Ley N° 19.799, sobre Documentos Electrónicos, Firma Electrónica y la Certificación de dicha Firma, del entonces Ministerio de Economía, Fomento y Reconstrucción, actual Ministerio de Economía, Fomento y Turismo.

METODOLOGÍA

El estudio se practicó de acuerdo con lo establecido en la resolución N° 20, de 2015, que fija normas que regulan las auditorías efectuadas por la Contraloría General de la República, y los procedimientos contenidos en la resolución exenta N° 1.485, de 1996, de este origen, que Aprueba Normas de Control Interno de la Contraloría General, e incluyó comprobaciones selectivas de los registros y la aplicación de otras pruebas, en la medida que se

estimaron necesarias. Asimismo, se efectuó un examen de cuentas a las transacciones relacionadas con los convenios de servicios tecnológicos.

Cabe precisar que las observaciones que la Contraloría General formula con ocasión de las fiscalizaciones que realiza se clasifican en diversas categorías, de acuerdo con su grado de complejidad. En efecto, se entiende por Altamente Complejas/Complejas, aquellas observaciones que, de acuerdo a su magnitud, reiteración, detrimento patrimonial, eventuales responsabilidades funcionarias, son consideradas de especial relevancia por la Contraloría General; en tanto, se clasifican como Medianamente complejas/Levemente complejas, aquellas que tienen menor impacto en esos criterios.

UNIVERSO Y MUESTRA

De acuerdo con la información proporcionada por la Comisión Nacional de Riego, durante el período revisado se administraron 71 contratos de carácter tecnológico, con un monto total pagado, a la fecha de revisión, de $ 344.681.052.

Las partidas sujetas a validación se seleccionaron analíticamente, considerando tres convenios, servicio de mantención y testing UNIBOX; el proyecto del Sistema Electrónico Ley 18.450 y el Enlace MPLS[1] de 20 Mb de Interconexión Santiago, La Serena, Temuco y Chillán, suscritos con las empresas Sociedad de Tecnologías de la Información Exceed Ltda.; Computación e Ingeniería S.A., y Claro Servicios Empresariales S.A., respectivamente, equivalentes a $ 85.212.198, que corresponde al 24,7% del universo antes indicado, según se presenta en la siguiente tabla:

Tabla N° 1: Resumen de convenios correspondientes al muestreo no estadístico.

MATERIA ESPECÍFICA	UNIVERSO		MUESTRA NO ESTADÍSTICA		TOTAL EXAMINADO	
	$	N°	$	N°	$	N°
Contratos de servicios informáticos.	344.681.052	71	85.212.198	3	85.212.198	3

Fuente: Antecedentes suministrados vía correo electrónico de 5 de febrero de 2016, del Coordinador de la Unidad de Soporte Informático de la CNR, respecto a las contrataciones vigentes durante el período en análisis.

Adicionalmente, a través del correo electrónico de 5 de febrero de 2016, del Coordinador de la Unidad de Soporte Informático, la institución auditada comunicó que posee 24 servidores físicos localizados en el datacenter de la CNR, en la Región Metropolitana, los que fueron validados en un 100%:

1 MPLS: Siglas de Multiprotocol Label Switching, es un mecanismo de transporte de datos estándar, que opera entre la capa de enlace de datos y de red.

Tabla N° 2: Resumen del universo de servidores informáticos y la muestra no estadística examinada.

MATERIA ESPECÍFICA	UNIVERSO		MUESTRA NO ESTADÍSTICA		TOTAL EXAMINADO	
	$	N°	$	N°	$	N°
Servidores informáticos de la CNR.	0	24	0	24	0	24

Fuente: Información proporcionada mediante correo electrónico de 5 de febrero de 2016, del Coordinador de la Unidad de Soporte Informático de la CNR.

La información relativa a los comprobantes de pago asociados a los contratos vigentes durante el período en revisión fue puesta a disposición de esta Contraloría General, por medio de correo electrónico de 4 de abril de 2016, del Jefe del Departamento de Administración y Finanzas de la Comisión Nacional de Riego.

RESULTADO DE LA AUDITORÍA

Del estudio practicado, se determinaron las siguientes situaciones:

I. ASPECTOS DE CONTROL INTERNO

1. Ausencia de seguimiento de las observaciones emanadas de la auditoría externa realizada por la empresa Decalink Ltda.

Se evidenció que la Unidad de Auditoría Interna de la repartición fiscalizada no ha realizado un seguimiento a las observaciones emanadas del Informe Final N° if00120141, de 28 de febrero de 2014, sobre Auditoría del Sistema Electrónico Ley 18.450, ejecutada por la empresa Desarrollo Evaluación Control y Asesorías Ltda.

Lo anterior no guarda armonía con el principio de control previsto en el artículo 3°, inciso segundo, de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado. De igual forma, no se aviene con lo señalado en la letra e) del capítulo III, de la antes aludida resolución exenta N° 1.485, de 1996, de esta Contraloría General, que señala, en lo que interesa, que los directivos deben vigilar continuamente sus operaciones y adoptar inmediatamente las medidas oportunas ante cualquier evidencia de irregularidad o de actuación contraria a los principios de economía, eficiencia o eficacia.

El servicio en su respuesta señala que, en relación al hallazgo descrito, la Unidad de Auditoría Interna, en el marco del Plan Anual del año 2014, emitió el informe N° 16, de 27 de noviembre de la citada anualidad, sobre auditoría al proceso concursal de la ley N° 18.450, del cual se consideraron los hechos presentados para llevar un seguimiento del trabajo realizado por las distintas áreas involucradas, recomendando a la autoridad de la repartición, extender el trabajo de ese equipo en lo que respecta al mantenimiento del actual

sistema, y el levantamiento de requerimientos necesarios para la implementación de una nueva plataforma electrónica de postulación y seguimiento, tomando en consideración los procedimientos que la Unidad de Soporte Informático confeccionó en el marco del Sistema de Gestión de Calidad.

Añade, que en las auditorías realizadas por la Unidad de Auditoría Interna, se validó la realización de un análisis para el año 2015 relativo al Sistema de Seguridad de la Información, SSI, bajo la norma ISO 27.000, que se incorporaba al Sistema de Gestión de la Calidad, SGC, y de cuyo resultado se gestó un plan de mejoras a ser ejecutado con recursos presupuestarios del año 2016 donde, entre otras acciones a efectuar, se encontraba el mejoramiento de la seguridad del datacenter y la realización de pruebas al plan de contingencia.

En consideración a la revisión efectuada a los antecedentes suministrados por la repartición, que evidencian un seguimiento a las observaciones emanadas por la empresa Decalink Ltda., respecto al Sistema Electrónico Ley 18.450, se levanta lo advertido preliminarmente.

2. Falta de estipulación contractual para la prestación relativa a enlace de datos MPLS.

Del análisis de los antecedentes que respaldan los Servicios de Transmisión de Datos MPLS, contratados por la CNR a través de la orden compra ID N° 870-441-SE14, se advirtió que la entidad no estipuló una fecha de recepción de la prestación, con el fin de hacerla exigible y evitar dilaciones innecesarias, afectando con ello el principio de eficacia previsto en el artículo 3° de la ley N° 18.575.

Respecto a esta materia, la organización fiscalizada señala en su respuesta que las compras realizadas a través del convenio marco se regulan por las condiciones y obligaciones del referido acuerdo y de las bases de licitación que la originan, según lo indicado en el artículo 18 del decreto N° 250, de 2004, del Ministerio de Hacienda, que aprueba el reglamento de la ley N° 19.886, de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios.

En atención a lo descrito por el servicio, es del caso precisar que la resolución exenta N° 1.514, de 23 de mayo de 2014, en el punto 2 de las especificaciones técnicas, describe que "El servicio debe ser instalado y entregado 30 días después de ser adjudicado el contrato al operador.", situación que permite levantar lo objetado.

II. EXAMEN DE LA MATERIA AUDITADA

1. Falta de mecanismos de revisión periódica a la integridad de la información.

Se verificó la existencia de modificaciones directas efectuadas a la información almacenada en la base de datos productiva del

Sistema Electrónico Ley 18.450, las cuales tienen relación con el ingreso, borrado y actualización de datos, poniendo en riesgo su integridad.

Sobre la materia, en declaración prestada ante personal de esta Contraloría General, don Pablo Asenjo Castro, encargado del aludido sistema, confirmó que entre las posibles consecuencias de una manipulación de la información gestionada en el sistema, se encuentran problemas de integración e inconsistencia de datos, visualización, y en la medida en que se modifiquen índices internos, la no disponibilidad del servicio.

A su turno, doña Olga Oriana Barahona, profesional de apoyo del Departamento de Fomento al Riego, que actualmente efectúa modificaciones en la base de datos productiva del sistema, declaró no poseer estudios formales que avalen su capacidad técnica para la administración de ésta, reconociendo que dicha habilidad fue adquirida de forma autodidacta a medida que se iba construyendo dicho aplicativo. Adicionalmente, señaló que para efectuar modificaciones a los datos, utiliza un conjunto de consultas preestablecidas en SQL[2], que ha ido elaborando de manera individual con el transcurso de los años.

Complementariamente, la mencionada funcionaria declaró no ejecutar actualizaciones masivas de los datos, ni la eliminación de estos en el sistema, debido a que este tipo operaciones posee mayor complejidad.

Conforme lo anterior, no se advierte la existencia de procedimientos y de reportes que permitan evaluar la integridad de la información contenida en el referido sistema, lo que transgrede lo establecido en el artículo 23 del decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, ya mencionado, sobre gestión de las operaciones y las comunicaciones.

Con respecto a esta materia, la entidad auditada indica en su respuesta que, a junio de 2016, no se cuenta con un procedimiento escrito, sin embargo, la elaboración de la memoria anual del departamento y de los reportes mensuales entregados a las distintas áreas de la CNR, exige una revisión de la integración de los datos de los años anteriores, controlando y manteniendo la integridad de la información relevante.

Debido a que lo informado por el servicio confirma la inexistencia del correspondiente mecanismo, asociado a la información almacenada por el Sistema Electrónico Ley 18.450, se mantiene lo observado.

2. Omisión de pruebas al plan de continuidad del negocio.

Se detectó que el servicio no cuenta con un registro de pruebas realizadas al plan de contingencia, en relación con la sala de servidores, infringiendo lo instituido en la letra i), del artículo 37, del decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, que dispone el nivel avanzado de seguridad del documento electrónico.

---

2 SQL: Lenguaje de consulta estructurada por instrucciones que permiten seleccionar, insertar, actualizar y eliminar información de la base de datos, entre otras funcionalidades.

La repartición auditada, en su respuesta, señala que la Unidad de Soporte Informático se comprometió con ejecutar 2 pruebas durante el año 2016, con el fin de comprobar la efectividad del plan de contingencia relacionado con la infraestructura TI en la CNR. Dicho compromiso fue adoptado a nivel de cumplimiento del Convenio de Desempeño Colectivo Institucional, aprobado mediante resolución exenta N° 4.819, de 14 de diciembre de 2015.

Sin prejuicio que lo informado por el servicio contempla la ejecución de pruebas, la vulneración se refería a la ausencia de registros de estas, lo que fue corroborado por la institución, manteniéndose lo advertido.

3. Carencia de un programa de actualización al plan de contingencia.

El Plan de Contingencia Informático de la entidad no posee un programa de gestión de cambios, lo cual se advierte en el numeral 8, el que versa sobre el Sistema de Información Geográfica ESSIR, apartado en el que se hace mención a un contrato vigente que finalizó en abril de 2012, vulnerando así lo dispuesto en la letra i), del artículo 37 del decreto N° 83, de 2004, antes citado.

Para el hallazgo comunicado, la CNR en su respuesta señala que, si bien existe un contrato que finalizó en el año 2012, actualmente el aprobado mediante las resoluciones exentas N^{os} 2.013 y 1.809, de 4 de julio de 2014 y 29 de abril de 2015, respectivamente, brinda mantención y soporte al sistema ESSIR.

Debido a que lo informado por la repartición auditada ratifica la desactualización del aludido plan en cuestión, dado que este no registra el precitado contrato, manteniéndose lo objetado preliminarmente.

4. Falta de controles físicos considerados en el procedimiento de control de acceso a la sala de servidores.

Mediante oficio ORD. N° 228, de 22 de enero de 2016, se suministró el procedimiento de control de acceso al datacenter de la CNR, el cual no considera dentro de su estructura, la necesidad de registrar por escrito el propósito de la visita y el uso obligatorio del carné de identidad como medio de identificación válida en el caso de los chilenos, y el pasaporte para extranjeros, incumpliendo lo señalado en la letra e), del artículo 37 del decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, el cual dispone el nivel avanzado de seguridad del documento electrónico.

La CNR en su respuesta señala que, si bien existe un registro del control de acceso a la sala de servidores, durante el mes de abril se iniciaron las gestiones necesarias para rediseñar un nuevo registro de visitas que refleje el propósito de esta, y que se impartirán las instrucciones necesarias para exigir la identificación de carné de identidad o pasaporte, según sea el caso.

Del análisis de lo descrito por la comisión, y de la visita efectuada al datacenter institucional el 10 de junio de 2016, se constató que las precitadas medidas no se han implementado, por lo que se mantiene lo observado.

5. Debilidades en el control de acceso a redes externas.

En relación con las pruebas efectuadas mediante el uso de un equipo computacional configurado en la red interna como de uno externo conectado a la misma, se evidencia una falta de resguardo relativa a la restricción de acceso a sitios externos, dada la factibilidad de interacción con sitios web que administran contenido no confiable en internet.

Dicha situación afecta el principio de control previsto en el artículo 3° de la ley N° 18.575.

La entidad fiscalizada señala en su respuesta, que la factibilidad de interacción con sitios externos es permitida dentro de la CNR, después de un análisis del tráfico de red interno y enmarcado dentro de las atribuciones del servicio para administrar los bienes a su cargo. Agrega que el control permanente del acceso es gestionado a través de un reporte ejecutivo semanal, el cual se obtiene desde la plataforma central de McAfee[3], que realiza un monitoreo permanente de la navegación de los usuarios, a lo que se suma una serie de resguardos a nivel de firewall, que bloquean la navegación a sitios con contenido no confiable.

Del estudio realizado a los antecedentes entregados, no se pudo evidenciar la existencia de acciones correctivas concretas para las situaciones descritas, dado que el aludido documento solo entrega información relativa al consumo de ancho de banda, separando por categoría, respecto a cuáles son las que presentan mayor consumo y los usuarios con mayor cantidad de tráfico en estas, junto con un enfoque en la categoría de streaming[4], por lo que lo advertido se mantiene.

6. Ausencia de estrategias de recuperación ante desastres.[5]

Del análisis efectuado a la información disponibilizada por medio del oficio ORD. N° 2.648 de 19 de agosto de 2015, se comprobó que el Plan de Contingencia Informático de la repartición auditada, no contempla dentro de su estructura, estrategias destinadas a la recuperación ante desastres de los sistemas críticos institucionales, contraviniendo lo previsto en el artículo 35, del decreto N° 83, de 2004, el cual dispone la gestión de la continuidad del negocio.

---

3 McAfee: Compañía de software especializada en temas sobre seguridad informática.
4 Streaming: Distribución digital de multimedia a través de una red de computadoras, de manera que el usuario consume el producto mientras que este se descarga.
5 Estrategias de recuperación ante desastres: Corresponden a los procesos prácticos de recuperación, cubriendo datos, hardware y software crítico, para que un negocio pueda comenzar de nuevo sus operaciones, en caso de desastres naturales u otros ocasionados por errores humanos.

La repartición auditada, en su respuesta, señala que dicho plan alude en el párrafo 3 de su capítulo IV, sobre estrategias, que cuando ocurre una contingencia, se procederá en el menor tiempo posible a determinar cuáles fueron las causales que originaron la emergencia y el posible daño que esta pudiera haber causado, con el fin de recuperar la continuidad del proceso o servicio. De ser necesario, en primer lugar, se recurrirá a los proveedores de soporte y mantención contratados, o en su defecto, a cualquier especialista o técnico que posea las competencias correspondientes.

Del análisis efectuado a los nuevos antecedentes suministrados por la CNR, se evidenció que a nivel individual, no todos los sistemas poseen acciones correctivas asociadas a su recuperación, por lo que se mantiene lo objetado.

7. Carencia de una política que instruya sobre el uso del correo electrónico institucional.

A través del correo electrónico de 29 de enero de 2016, el Encargado de Seguridad de la Información de la CNR, suministró políticas y procedimientos relativos al Sistema de Seguridad de la Información, SSI, en las cuales se acreditó la omisión de la política que regula el uso y distribución de correos electrónicos, transgrediendo lo instruido en la letra b), del artículo 20, del decreto N° 83, de 2004, la cual dispone la seguridad del personal.

La Comisión Nacional de Riego en su respuesta señala que, si bien en las inducciones se contemplan el cuidado que los funcionarios deben tener respecto al uso de la red interna, de internet, del correo electrónico y acceso a servicios públicos de recursos compartidos, servicios de mensajería y comunicación remota, este será formalizado en el procedimiento de alta de usuarios de la institución.

Debido a que lo informado por la entidad auditada contempla medidas correctivas, que a la fecha de elaboración del presente informe final, no han finalizado, se mantiene lo observado.

8. Falta de un proceso formal de inducción a las medidas de seguridad TI adoptadas por la institución.

Del análisis realizado a la información suministrada vía correo electrónico de 4 de febrero de 2016, del Encargado de la Seguridad de la Información, se constató que no existe un programa de inducción formal para los funcionarios de TI, sobre los procesos y procedimientos de emergencia acordados en los planes de continuidad del negocio, incluyendo una crisis de dirección, lo que no se encuentra en concordancia con lo preceptuado en el literal i), del artículo 37 del decreto N° 83, de 2004, la cual dispone el nivel avanzado de seguridad del documento electrónico.

Al respecto, la repartición indica en su respuesta que, en el marco del Programa de Buenas Prácticas Laborales comprometidas con el Servicio Civil, se encuentra trabajando en la actualización y

mejora de la Política de Personas, donde se está incorporando el Programa de Inducción Institucional. Agrega que, en dicho apartado, se incorporará la inducción específica para el cargo, en el caso de los funcionarios del área de TI, la cual contendrá la relativa a materias de seguridad.

Asimismo, la institución fija el 30 de junio de 2016 como el plazo máximo para que el Programa de Inducción Institucional se encuentre aprobado.

En circunstancia que lo informado por la CNR ratifica la carencia del proceso de inducción formal de esta índole, y que no consta la solución efectiva de esa falencia, se mantiene lo advertido.

9. Falta de seguridad en el sitio externo de almacenamiento.

De la revisión efectuada a la bodega de archivos de la CNR, ubicada en [redacted], se constató la existencia de una caja fuerte que almacena las cintas de respaldo con la información administrada de la repartición, la cual carece de anclaje y medidas de seguridad anti incendio.

En lo relativo al espacio físico, se observó la existencia de material inflamable, debido a que el propósito principal de este depósito es custodiar documentación en papel administrada por la CNR, poniendo en riesgo la seguridad de los respaldos.

Complementariamente, si bien el acceso a esta área es restringida a personal debidamente autorizado, haciendo uso de una llave de acceso o combinación numérica, esta última medida atenta contra quien ingresa a esta dependencia, ya que al hacer uso de este último método, no existe una alternativa de evacuación, si no se posee la llave.

Se evidencia una red de cañerías en el cielo de dicha habitación, las que al ser activadas ante eventos de combustión presentes en la sala de respaldos, presentan un riesgo para los activos de back up.

Lo manifestado, vulnera la letra d), de artículo 24 del decreto N° 83, de 2004, sobre la gestión de las operaciones y las comunicaciones.

El servicio, en su respuesta, señala que estudiará alternativas de resguardo en otro edificio del Ministerio de Agricultura, que cumpla con las condiciones de seguridad, o bien, considerará una alternativa de arrendamiento especializado, en la medida que se disponga de los recursos financieros necesarios para concretarlo.

Debido a que lo informado por la institución auditada contempla medidas correctivas a futuro, se mantiene lo objetado.

10. Uso de software no licenciado.

A través de correo electrónico de 5 de febrero de 2016, el Coordinador de la Unidad de Soporte Informático suministró el inventario de licencias de software gestionadas por la CNR, comprobándose el uso indebido de licencias asociadas al Sistema de Gestión Documental, dada la existencia de un total de 41 licencias, de las 20 contratadas, lo cual infringe lo anotado en los artículos 3° y 19, en relación con la naturaleza y objeto de la protección y el derecho patrimonial general, respectivamente, de la ley N° 17.336, sobre Propiedad Intelectual.

La entidad auditada informa, en síntesis, en su respuesta que el aludido sistema posee un tipo de licencia que permite la instalación de la citada plataforma en la cantidad de computadores que la CNR estime conveniente y solo se limita la cantidad de usuarios que pueden estar conectados de forma simultánea.

De acuerdo a lo señalado por la institución, es del caso indicar que la comisión proporcionó a esta Contraloría la oferta económica hecha por la empresa adjudicataria, Adquisiciones y Servicios Grupo Norte Limitada, que describe que las licencias ofrecidas son del tipo concurrente, lo que se condice con lo defendido por la CNR, por lo que se levanta lo advertido.

11. Uso de software descontinuado y sin soporte.

Considerando el inventario de licencias de software administradas por la repartición, se advirtió el uso de software ofimático obsoleto, lo que se aparta de lo consagrado en el literal 12.4.1, de la Norma Chilena NCh-ISO 27.002, del Instituto Nacional de Normalización de Chile, sobre seguridad de los archivos del sistema.

La CNR en su respuesta informa que, en la práctica, las estaciones de trabajo y equipos portátiles cuentan con licencias ofimáticas instaladas en sus versiones 2013 y 2016 (Microsoft Office 365), tal como el resto del software de soporte y de productividad, encontrándose ciertas discrepancias en la información contenida en el inventario, pero sin afectar la seguridad de los aplicativos institucionales.

Complementariamente, consigna que el sistema de activo fijo Softland[6] está siendo reemplazado por el sistema Ungasoft[7], proceso que requerirá la actualización de inventario.

Debido a que la citada norma chilena tiene por objeto establecer recomendaciones y principios generales para iniciar, implantar, mantener y mejorar la gestión de la seguridad de la información en una organización,

6 Softland: Compañía que pertenece al holding tecnológico Grupo Softland, la cual provee de soluciones de gestión administrativa empresarial, tales como software ERP.
7 Ungasoft: Compañía que comercializa e implementa software encargado de las áreas de administración de infraestructura computacional, activos fijos, mesas de ayuda, manejo de correspondencia, abastecimiento e inventario.

cabe anotar que lo señalado en este numeral no constituye una observación propiamente tal.

12. Autentificación débil en el Sistema Electrónico Ley 18.450.

Conforme a las pruebas efectuadas en el citado sistema, se detectó la asignación de contraseñas con longitud inferior a ocho caracteres, no alfanuméricas, con letras y números consecutivos, lo que infringe lo dispuesto en la letra g), del artículo 28 del decreto N° 83, de 2004, ya mencionado, sobre el control de acceso.

Cabe señalar que el inciso final del referido artículo 28 indica que los sistemas computacionales deberán configurarse de manera que los usuarios se vean compelidos a cumplir con las obligaciones impartidas sobre seguridad de los documentos electrónicos.

Al respecto, la entidad en su respuesta indica que, si bien en un inicio el aplicativo no consideraba las exigencias establecidas en la citada normativa, en lo relativo a la creación de claves, al momento de la auditoría la plataforma exigía los elementos de seguridad recomendados.

Relativo a los casos detectados, menciona que estos corresponden a usuarios vigentes con claves antiguas, quienes solo podrán ingresar, en la medida que actualicen sus claves de acuerdo a los nuevos parámetros de seguridad ya referidos. En otras palabras, el sistema antes de hacer cualquier operación obliga a estos usuarios a cambiar la contraseña por una que entregue los elementos de seguridad mencionados.

En razón a que el correo electrónico de 10 de febrero de 2016, que hizo entrega de las credenciales de acceso para que esta Contraloría pudiese llevar a cabo el análisis del software, evidencia el no cumplimiento de los estándares mínimos requeridos que deben cumplir las contraseñas, y que además, haciendo uso del sistema en el periodo auditado, se comprobó la no existencia de la funcionalidad que obliga el cambio de esta, se mantiene lo observado.

13. Falta de revisión de los permisos de acceso.

Por medio de correo electrónico de 5 de febrero de 2016, el Coordinador de la Unidad de Soporte Informático suministró el procedimiento denominado Gestión de Acceso a Redes Locales y Servicio Mensajería Electrónica, el cual establece los procesos relativos al alta y baja de los usuarios en los diversos sistemas de información de la CNR. Además, instruye una frecuencia a lo menos semestral de comprobación de los derechos de acceso de la repartición, recayendo la responsabilidad en el Analista de Infraestructura o quien le reemplace.

Tras el análisis realizado a la base de datos del Sistema Electrónico Ley 18.450, se acreditó la presencia de cuentas vigentes de personal desvinculado hace ya más de un semestre, vulnerando lo establecido en la letra g), del artículo 37 del decreto N° 83, de 2004, sobre el control de acceso, ver Anexo N° 1.

El servicio, en su respuesta, señala que detallará las responsabilidades de la Unidad de Soporte Informático y de aquellas que administran los propios sistemas, en lo que respecta al proceso de alta y baja de usuarios.

En atención a que lo informado por la CNR no evidencia medidas correctivas orientadas a subsanar el hallazgo, se mantiene lo advertido.

14. Carencia de un registro de intentos de acceso fallidos al Sistema Electrónico Ley 18.450.

Conforme a las pruebas ejecutadas al precitado sistema, se corroboró la inexistencia de un registro de intentos de acceso fallidos, que contuviese la fecha, hora y el aviso al encargado de seguridad, lo que no se condice con lo mencionado en el acápite 11.5.1, de la Norma Chilena NCh-ISO 27.002, de 2009, del Instituto Nacional de Normalización de Chile, sobre procedimientos de conexión segura.

La organización auditada, en su respuesta indica que, si bien no existe un registro de intentos fallidos de acceso al sistema, en la que se anote la fecha, hora y aviso al encargado de seguridad, sí se cuenta con registros dentro de la base de datos que almacenan la fecha y hora del intento de acceso, la IP de la conexión, el identificador del usuario que intenta conectarse, así como si el evento es un acceso no autorizado o desconexión del sistema, siendo estos registros utilizados para hacer un seguimiento y análisis de la trazabilidad relativa al ingreso de información al aplicativo.

De manera complementaria, señala que la seguridad en cuanto a ataques a los servicios web de la CNR se encuentra monitoreada por empresas de soporte externas, permitiendo tener un control de acceso a nivel de infraestructura de la red institucional.

Sin perjuicio que las medidas informadas por la institución contemplan acciones de control orientadas a mitigar la debilidad detectada, debe precisarse que la citada norma chilena tiene por objeto establecer recomendaciones y principios generales para iniciar, implantar, mantener y mejorar la gestión de la seguridad de la información en una organización, por lo que lo anotado en este numeral no constituye una observación propiamente tal.

15. Deficiencia en el control y gestión del inventario TI.

Del examen practicado al inventario de los bienes TI, relativo a 24 servidores físicos de la entidad, ubicados en las salas de servidores primaria y secundaria, provistas por la Oficina de Estudios y Políticas Agrarias, ODEPA, y la Comisión Nacional de Riego, respectivamente, no se pudo constatar en terreno la existencia de sus bienes inventariados, producto de la inconsistencia de los códigos presentes en los componentes electrónicos respecto de los contenidos en el inventario institucional de la CNR, lo que transgrede lo señalado

en la letra c), del artículo 37 del decreto N° 83, sobre la clasificación y el control de bienes, cuyo detalle se presenta en el Anexo N° 2.

Al respecto, la CNR consigna que el módulo de activo fijo de Softland[8], está siendo reemplazado por el sistema Ungasoft, proceso que requerirá la actualización de inventario y que, a su vez, corregirá las inconsistencias entre el registro institucional y el informático.

Dado que el servicio confirma la falta de integridad de su inventario en estudio en tanto la medida que informa no ha concluido, se mantiene lo observado.

16. Falencias en el control de acceso al Sistema Electrónico Ley 18.450.

Se comprobó que el actual sistema permite el ingreso de usuarios no registrados a la plataforma, a través de un cambio de parámetro presente en el enlace que provee el módulo de recuperación de contraseña para los usuarios registrados en dicho aplicativo. Para mayor detalle remitirse a la información contenida en el Anexo N° 3.

La citada brecha de seguridad infringe lo previsto en la letra g) del artículo 37 del decreto N° 83, sobre el control de acceso.

El servicio en su respuesta señala que, si bien al ingresar a la opción de recuperar contraseña un usuario no registrado puede cambiar un parámetro de la URL[9] vinculado a la visualización de un determinado menú dentro del sistema, este cambio solo admite ingresar a la opción de ingreso de un ticket de soporte o una solicitud de alta, sin tener acceso a la información dentro del sistema.

Adicionalmente, se compromete a evaluar la manera en que el sistema no acepte la manipulación de variables contenidas en la URL, aunque dichos controles ya se incorporan en la nueva versión del sistema.

Debido a que la CNR corrobora la existencia de la brecha de seguridad expuesta precedentemente, se mantiene lo advertido; además, en las pruebas realizadas por esta Entidad de Control, se pudo acceder al perfil de administrador, mediante los pasos señalados en el Anexo N° 4.

17. Ausencia de controles que restrinjan el cambio de perfilamiento.

Mediante el uso de la plataforma del Sistema Electrónico Ley 18.450, se evidenció la carencia de controles asociados a la asignación de perfiles de acceso, producto que cualquier persona puede acceder y modificar sus privilegios a otros que no han sido autorizados por sistema, logrando

8 Módulo de activo fijo de Softland: Permite llevar un control exhaustivo de los bienes del activo fijo, controlando cada uno de ellos, tanto en la ubicación que se encuentran, como la cantidad existente, las revalorizaciones, depreciaciones, valor libro, entre otras.
9 URL: Del inglés, Uniform Resource Locator, es un identificador de recursos uniforme, utilizado para acceder a sitios de internet.

inclusive ser administrador de la plataforma, vulnerando así lo establecido en la letra g), del artículo 37 del decreto N° 83, de 2004, sobre control de acceso.

En relación al hecho objetado, la entidad auditada menciona que, de acuerdo a su propia información y realizando pruebas de acceso tanto para usuarios registrados como mediante la opción de recuperación de contraseña, no se logró el ingreso al mantenedor de perfiles de usuario, no siendo posible, a su entender, que un usuario, al efectuar un cambio de parámetro en la URL, ya sea variando el parámetro de opción o agregando el nombre de la página, tenga acceso a cambiar su rol.

Considerando que el preinforme de observaciones N° 305, no acreditó gráficamente este hallazgo, solicita a este Ente Contralor indicar de qué manera esto se constató, con el fin de tomar las medidas correctivas necesarias para poder subsanar lo expuesto.

En relación a lo expuesto precedentemente, cabe mencionar que la ausencia de controles relativos al cambio de perfilamiento podría repercutir en el mal uso de las atribuciones que el administrador del sistema posee, así como conllevar a la competencia desleal de parte de consultoras que tengan acceso a las variables de postulación de sus contrincantes antes de la fecha apertura. En cuanto a las pruebas desarrolladas por esta Entidad de Control, ellas se presentan en el Anexo N° 4.

Dado que lo expresado por la CNR no suministró respaldos que permitan evidenciar la aplicación de medidas correctivas orientadas a subsanar esta vulnerabilidad, se mantiene lo advertido.

18. Falta de controles de acceso a información confidencial de proyectos.

Respecto del análisis efectuado al sistema, se corroboró que, por medio del uso de ataques informáticos orientados a la inyección de código ejecutable en la capa lógica de la aplicación, se accede a toda la información almacenada en la base de datos, quedando expuesta la de carácter confidencial de los concursos y usuarios de la plataforma, lo que contraviene lo dispuesto en la letra b), del punto 1.2, del artículo primero transitorio, del decreto N° 14, de 2014, del Ministerio de Economía, Fomento y Turismo.

La Comisión Nacional de Riego, en su respuesta, confirma la falla en el sistema, complementando que el proyecto en construcción del nuevo Sistema Electrónico Ley 18.450, contempla dentro de su estructura la implementación de medidas destinadas a mitigar la explotación de ataques informáticos, tales como SQLi[10] y XSS[11], apoyándose en las funcionalidades que provee la nueva herramienta de desarrollo.

10 SQLi: Método de infiltración de código malicioso que se sustenta en vulnerabilidades informáticas presentes a nivel de validación de las entrada de una aplicación, a fin de realizar operaciones sobre su base de datos que permitan la adquisición de información confidencial contenida en esta.

Sobre lo informado, cabe mencionar que dicha brecha de seguridad expone en su totalidad al sistema, permitiendo entre otras cosas, la obtención de credenciales de acceso, suplantando la identidad de usuarios para fines propios; conocer los valores de variables asociados a los proyectos postulados a concursos, antes de la fecha de apertura; y que, junto con la suplantación de identidad, permite la modificación, eliminación y actualización de información sensible de la base de datos, poniendo en riesgo la integridad de la información del sistema.

Considerando que la repartición confirma el hallazgo, y que no evidencia medidas correctivas al corto plazo para subsanar esta vulnerabilidad, se mantiene lo objetado preliminarmente.

19. Deficiencia de controles de acceso a la base de datos.

A través de la evaluación realizada al aplicativo, se advirtió la existencia de una interfaz en el perfil de administrador, que permite insertar, eliminar y actualizar la información almacenada en la base de datos productiva de la plataforma.

Asimismo, la señora Olga Barahona Saldías, en su declaración del 4 de abril de 2016, expuso que cuando cumplía el rol de encargada de concursos, no poseía acceso a la precitada base, y que solo se le habilitó una vez que el Departamento de Fomento al Riego se hizo cargo de dicho aplicativo.

Por otro lado, vía correo electrónico de 7 de abril de 2016, la aludida funcionaria se contradice, al afirmar que ha tenido la funcionalidad habilitada desde el año 2012.

Además, manifestó que el responsable de la creación de dicho componente del sistema fue don Sebastián Casabonne Vilches, profesional de apoyo del Departamento de Fomento al Riego, a requerimiento del Departamento de Fomento al Riego, cuyo propósito era, en principio, proveer de una mayor cantidad de "mantenedores del sistema"[12].

Adicionalmente, don Pablo Asenjo Castro, Administrador del Proyecto Sistema Electrónico Ley 18.450, a través de correo electrónico del 7 de abril de 2016, corroboró que el acceso y uso del aludido formulario solo está permitido a aquellos usuarios que poseen autorización para utilizar el perfil de administrador, y que las modificaciones a los datos mediante esta funcionalidad implican el registro tanto de las acciones efectuadas como del usuario responsable de dichas operaciones.

---

11 XSS: Ataque informático que se aprovecha de un fallo en el sistema de validación de HTML incrustado y consiste en inyectar código ejecutable donde no debería existir, con el fin de conseguir algún provecho del atacante.
12 Mantenedores del sistema: Formulario en donde se puedan insertar, eliminar y actualizar los datos productivos de la plataforma.

Complementariamente, don Sebastián Casabonne Vilches confirmó lo expuesto en el párrafo precedente, manifestando que a dicho menú solo pueden acceder usuarios administradores del sistema, y que el propósito de la interfaz es ingresar, actualizar y borrar la información de la base de datos productiva, registrando las operaciones ejecutadas. Del mismo modo, expresó que su uso requiere de conocimientos del modelo de base de datos y del flujo del proceso del negocio, haciendo imposible, a su juicio, que un usuario cualquiera pueda operarlo.

Al tenor de lo señalado y del análisis de los registros de cambios efectuados en la aludida base de datos, se evidenció que la funcionaria Olga Barahona Saldías ha efectuado continuas modificaciones a los datos contenidos en el sistema en estudio.

Lo antes mencionado, afecta los principios de eficiencia, eficacia y control, previstos en los artículos 3° y 5° de la ley N° 18.575.

La Comisión Nacional de Riego, en su respuesta, señala que los cambios realizados por la profesional encargada a través de la mencionada interfaz, apuntan -precisamente- a mantener la integridad de la información entregada por los proyectos postulados a concurso, de forma de mantener la coherencia entre la información enviada a través de formularios y certificados, y la información digitada en la plataforma.

De forma complementaria, indica que para mantener un registro de los cambios efectuados, toda modificación ejecutada se registra en la tabla llamada t_logquery, de forma de mantener una trazabilidad de las mismas.

Adicionalmente, se compromete a establecer un procedimiento en el cual el registro de los aludidos cambios sea revisado por la jefatura del Departamento de Fomento al Riego, o quien se designe para el caso, con el fin de tener un control interno a nivel institucional.

Considerando que la repartición contempla la creación de un nuevo procedimiento que permita fortalecer los controles internos existentes, lo cual confirma la debilidad evidenciada, por otro lado, que los argumentos presentados no justifican la asignación de permisos de rectificación de los datos del Sistema Electrónico Ley 18.450 para la aludida funcionaria, se mantiene lo observado.

20. Hallazgo de vulnerabilidad sin subsanación.

La empresa Cepia Ingenieros Consultores Ltda., notificó a la Comisión Nacional de Riego, a través de un correo electrónico de 10 de diciembre de 2013, que el sistema presentaba vulnerabilidades que permitían acceder a la información de otros proyectos presentados, ingresando al menú denominado postulación, oprimiendo en impresión de documentos y seleccionando el concurso. De igual manera se podía acceder, entre otros, al formulario único de postulación, en el cual se exponen los valores para el cálculo del puntaje y posterior asignación de bonos.

Asimismo, la indicada consultora adjuntó documentación que evidenciaba visualmente el modo en que ella pudo acceder a la información de un proyecto postulado en el concurso N° 25-2013.

Mediante correo electrónico de 23 de diciembre de 2013, la citada consultora notificó nuevas deficiencias del sistema, entre ellas, que un usuario que no posee acceso como consultor, ingrese a este.

Complementariamente, a través de la aludida declaración, doña Olga Barahona Saldías señaló que, en dicho período, el Departamento de Fomento al Riego analizó los avances de las soluciones aplicadas para regularizar tales falencias por parte del equipo compuesto por los señores Sebastián Casabonne Vilches, Pablo Asenjo Castro, Marcelo Parra Velásquez, ocasionalmente por don Claudio Camblor Aróstica, y ella, cumpliendo esa funcionaria el rol de supervisora en todo el proceso, para finalizar con la aprobación de su solución.

En relación a aquellas situaciones enunciadas por la consultora Cepia Ingenieros Consultores Ltda., don Pablo Asenjo Castro, el 4 de abril de 2015, efectuó una declaración a esta Entidad de Control, en la cual detalló que, dentro de las medidas adoptadas para mitigar dichos riesgos se considera el cifrado de la información por medio del uso de certificado, cambios en la configuración del servidor en donde se encuentra alojado el aplicativo y encriptaciones de los valores de los parámetros utilizados en la capa de presentación[13].

Al respecto, se constató que, tanto la vulnerabilidad descrita en el comunicado del 10 de diciembre de 2013, como la del correo electrónico del 23 de igual mes y año, no se encontraban regularizadas al 25 de abril de 2016, debido a que se accedió a la información de terceros.

Lo señalado, incumple los principios de eficiencia y eficacia previstos en los artículos 3° y 5° de la ley N° 18.575.

Sobre lo expuesto, el servicio en su respuesta informa, en síntesis, que mediante la orden de compra N° 870-20-CM14, de 31 de enero de 2014, se contrató a la Empresa de Ingeniería en Computación y Tecnologías, por 537 horas profesionales, la cual, en base a lo notificado por el consultor y bajo la supervisión de la CNR, modificó el código de toda la plataforma, con el fin de no permitir que mediante el cambio de parámetros en la URL, los usuarios registrados pudieran acceder a la información de otros proyectos a los cuales no debían tener acceso.

Debido que esta Contraloría verificó la obtención de la misma información confidencial que, en su momento, la aludida consultora denunció, y que la repartición en su respuesta menciona que estas

13 Capa de Presentación: Corresponde al nivel del modelo de interconexión de datos, encargado de manejar las estructuras de estos y realizar las conversiones necesarias para la interpretación de los mismos entre sistemas.

vulnerabilidades serán subsanadas en una nueva versión del software, se mantiene lo advertido.

21. Cierre de incidencia sin medida adoptada.

El 16 de noviembre de 2012 y bajo la plataforma Mantis, la cual administra los incidentes y requerimientos del citado sistema, se generó el ticket N° 318, informado por don Ismael Garrido Valdés, quien apoyaba en las tareas de implementación, desarrollo y soporte de sistemas de la CNR y asignado a Marcelo Parra Velásquez, encargado de gestionar proyectos y el desarrollo de la implementación, el mantenimiento y el soporte del Sistema Electrónico Ley 18.450, debido a un supuesto error que afectaba de manera transversal al aludido aplicativo, clasificado por el informante como de severidad mayor, el cual dentro de su descripción indicaba, entre otras cosas, que la metodología de programación era altamente insegura, debido a la cantidad de parámetros que el sistema visualizaba en la capa cliente[14], siendo cerrado según registro del sistema por el denunciante el 30 de agosto de 2013.

No obstante lo anterior, mediante correo electrónico de 5 de junio de 2013, don Pablo Asenjo Castro notificó a don Claudio Camblor Aróstica sobre la acción de limpieza de los incidentes y requerimientos ingresados al sistema Mantis, con el objetivo de contar con registros actualizados en dicha plataforma.

Por otra parte, a través de correo electrónico de 19 de febrero de 2014, don Marcelo Parra Velásquez informó a don Claudio Camblor Aróstica, que el Ticket N° 318 fue cerrado en la fecha en cuestión, a solicitud del Departamento de Fomento al Riego.

Lo expuesto, infringe lo indicado en la letra b) del artículo 12, del decreto N° 83, de 2004, sobre seguridad organizacional, y el artículo 11, de la ley N° 18.575, ya mencionada.

Al respecto, la Comisión Nacional de Riesgo en su respuesta señala que el referido ticket se refería a errores de ejecución en la aplicación, producto de una variable de entorno[15] erróneamente definida. En ese sentido, el error fue corregido al configurar de forma correcta el ambiente de ejecución, por lo que correspondía cerrar la incidencia.

Además, agrega que el antedicho ticket referencia que la metodología utilizada para programar el sistema podría, eventualmente, traer vulnerabilidades que no son posibles de subsanar en la actual versión del sistema; sin embargo, informa que la falencia advertida, será considerada dentro de la mejora de la nueva versión del Sistema Electrónico Ley 18.450.

14 Capa Cliente: Corresponde a aquella conformada por la lógica de la aplicación a la que el operador final accede directamente mediante una interfaz de usuario.
15 Variable de entorno: Concierne a un valor dinámico que normalmente afecta al comportamiento de los procesos en una computadora.

Es del caso hacer presente que la Comisión Nacional de Riego, en su respuesta, señala que tomó las medidas que, a su juicio, fueron las apropiadas, según los incidentes denunciados. Sin embargo, este Organismo de Control ha levantado una serie de observaciones que surgen a raíz del ticket N° 318, puesto que, como se señaló en su oportunidad, el mismo refleja que "la metodología de programación es altamente insegura, debido a que muestra muchos parámetros en la capa cliente, lo cual es información sensible que algún usuario podría mal utilizar", evento que produjo las vulnerabilidades citadas en los comunicados del 10 y 23 de diciembre de 2013, de parte de la empresa Cepia Ingenieros Consultores Ltda., y los hallazgos de los numerales 16, 17, 18, 20, 22, 23 y 24 del presente capítulo, por lo que se mantiene lo advertido.

22. Modificaciones en las variables de postulación posterior a la fecha de apertura.

La resolución exenta N° 586, de 3 de marzo de 2014, que aprueba la modificación al manual de procedimiento legal-administrativo de los concursos de la ley N° 18.450, en su punto 3.4, relativo a la postulación de proyecto, señala que "todo proyecto deberá indicar las variables de concurso de manera consistente en el Sistema de Postulación Ley N° 18.450 y en el formulario de postulación, no permitiendo sus modificaciones una vez realizada la apertura del concurso".

En base al análisis realizado por este Organismo de Control entre el 12 de febrero y el 25 de abril de 2016, a la información almacenada en la base de datos de dicho aplicativo, se evidenció que lo mencionado precedentemente no se encuentra en concordancia con lo reflejado en los datos, debido a la existencia de modificaciones realizadas a las variables de los proyectos postulados después de la fecha de apertura, en los concursos N^{os} 19-2014, 20-2014, 22-2014 y 23-2014, de 31 de julio los dos primeros, y 22 de agosto los dos últimos, todos del año 2014, lo que repercute en el resultado final de los certámenes.

Del análisis efectuado a la corrida de puntaje, considerando los valores de las variables de los proyectos postulados a concurso, en forma posterior a las modificaciones efectuadas después del período de apertura, no existen observaciones. No obstante, para los citados procesos concursales, se evidencian discrepancias al efectuar el aludido procedimiento previo a la fecha de apertura, tal como se indica en la citada resolución exenta N° 586, como se expone en el Anexo N° 5.

Asimismo, se observó la existencia de proyectos que fueron modificados en una o más variables fuera de plazo, conforme a lo respaldado en el Anexo N° 6.

Al tenor de lo expuesto, se advierte una transgresión de lo establecido en el punto 3.4 de la ya citada resolución exenta, debido a que los resultados obtenidos en la corrida de puntaje difieren de los obtenidos oficialmente por la CNR.

El servicio auditado en su respuesta señala que la modificación de costos en los aludidos concursos, se debió a un incidente

ocurrido al momento de la postulación de proyectos a concurso, mencionándose en el Informe de Avance Desarrollo de Requerimientos 2014.

En atención a que los antecedentes suministrados por la repartición solo detallan problemas en los datos respecto al concurso N° 19-2014, sin informar las autorizaciones de la dirección para ejecutar las modificaciones, ni clarificar las medidas adoptadas para que la situación planteada no se vuelva a repetir, se mantiene lo objetado preliminarmente.

23. Vulnerabilidades de seguridad informadas en la auditoría externa en el año 2014 y no subsanadas.

Por medio de la revisión de algunas de las falencias respaldadas en el Anexo N° 7, presentadas en el Sistema Electrónico Ley 18.450 durante el análisis efectuado por la empresa Decalink Ltda., las que fueron plasmadas mediante el informe N° if00120141, de 28 de febrero de 2014, se evidenció que, a la fecha de cierre de esta auditoría, no se habían realizado mejoras significativas en pos de subsanar esos hallazgos.

Lo anterior, vulnera lo establecido en la letra b), del artículo 12, del decreto N° 83, de 2004, sobre seguridad organizacional y lo señalado en la letra b), del punto 2, de la resolución exenta N° 3.689, de 24 de septiembre de 2015, de la Comisión Nacional de Riego, que nombra el encargado de seguridad de la información de la repartición.

La CNR, en su respuesta, menciona que la aludida auditoría externa fue solicitada para tener una opinión objetiva sobre el estado del Sistema Electrónico Ley 18.450, luego que se registró el incidente descrito en el numeral 20 de este capítulo, y que en dicho examen se recomendó el congelamiento de los desarrollos, centrándose solo en aquellas vulnerabilidades o necesidades que fueran relevantes.

Añade que, en ese sentido, se decidió subsanar la deficiencia descrita en el citado hallazgo, además de priorizar de forma consensuada algunos desarrollos internos, los que fueron finalizados en diciembre de 2014, luego de lo cual se congelaron los desarrollos en el aplicativo, a la espera de la implementación del nuevo sistema.

Considerando que la repartición no aportó antecedentes que acrediten la coordinación de la respuesta a incidentes computacionales por parte del encargado de seguridad conforme a la normativa vigente, se mantiene lo observado.

24. Sistema permite consultar datos de los postulantes a concursos a través del formulario de búsqueda.

Durante el período comprendido entre el 12 de febrero y el 25 de abril de 2016, se ejecutó una revisión al Sistema Electrónico Ley 18.450, utilizando el perfil de consultor, donde se evidenció que el formulario presente en el menú Postulación / Postulación / Impresión de Documentos, permite el ingreso

de comandos no autorizados, según consta en el Anexo N° 8, los cuales posibilitan listar los formularios de costos, superficie y postulación, además del certificado de postulación de todos los proyectos sometidos a concurso, incumpliendo la letra a) del artículo 6° y la letra g) del artículo 37, ambos del decreto N° 83, de 2004, sobre control de acceso y seguridad del documento electrónico en general.

La repartición en su respuesta corrobora lo indicado, expresando que el proyecto en construcción, que reemplazará el actual Sistema Electrónico Ley 18.450, contempla la no ejecución de código malicioso, en base a las opciones que posee la herramienta de desarrollo. En este sentido, y con la finalidad de resguardar la confidencialidad de la información, la primera parte del sistema en ser liberada, será la correspondiente a los consultores, de manera tal de impedir el acceso a la información almacenada en la base de datos.

Al tenor de lo expuesto, cabe señalar que la mencionada vulnerabilidad atenta contra la libre competencia en los procesos concursales, debido a que la información confidencial de las variables de postulación de las consultoras podría gatillar la modificación de las variables concursales, en forma anterior a la fecha de apertura, por parte de una empresa que desee obtener ventajas competitivas con respecto a sus contrincantes.

Considerando que la repartición confirma el hallazgo y no demostró la aplicación de medidas correctivas hasta la puesta en marcha del nuevo software, se mantiene lo advertido preliminarmente.

25. Falta de eficacia al contratar productos Red Hat para la creación de la nueva versión del Sistema Electrónico Ley 18.450.

A través de la ya aludida declaración de don Pablo Asenjo Castro, se evidencia que la contratación de productos Red Hat, con la empresa Computación e Ingeniería S.A., respaldada por las órdenes de compra ID N^{os} 870-965-CM14 y 870-981-CM14, de 23 y 30 de diciembre de 2014, respectivamente, tenía como propósito crear una nueva versión del Sistema Electrónico Ley 18.450. Sin embargo, debido a la falta de mano de obra dedicada a este proyecto y los antecedentes suministrados por el equipo del Departamento de Fomento al Riego, se resolvió el cese del proyecto.

Adicionalmente, por medio de correo electrónico de 24 de marzo de 2016, del Account Manager de Red Hat, se detectó que las suscripciones a los productos Red Hat JBoss BPM Suite 6 y JBoss Fuse Service Work, se encuentran inactivas desde el 15 de marzo de 2016.

Por otra parte, don Sebastián Casabonne Vilches, mediante correo electrónico de 19 de abril de 2016, confirmó que el ambiente

de JBoss no pasó a producción, quedando disponible solo para ambiente de desarrollo y QA[16].

Lo objetado no guarda armonía con el principio de eficacia, obligatorio para la Administración del Estado, previsto en los artículos 3° y 5° de la ley N° 18.575.

Al respecto, la institución auditada menciona en su respuesta que el hallazgo detectado corresponde a una parte del proyecto de creación del nuevo Sistema Electrónico Ley 18.450, y que si bien las suscripciones de los productos Red Hat no fueron renovadas, esto se produjo por una reestructuración del equipo de desarrollo interno, que se encuentra trabajando en la nueva versión del aplicativo, utilizando toda la infraestructura que se obtuvo para tales efectos.

Considerando que las acciones propuestas son de materialización futura y, a su vez, que la objeción expuesta es un hecho consolidado para la orden de compra ID N° 870-981-CM14, la cual no es susceptible de regularización, se mantiene lo objetado.

26. Funcionarios asignados como consultores en concursos.

Del análisis de la información almacenada en la base de datos del Sistema Electrónico Ley 18.450, se advirtió la existencia de irregularidades en la información relacionada, al menos, con los concursos 31-2015, 04-2014 y 07-2012, debido a la presencia de proyectos postulados a concurso por funcionarios de la Comisión Nacional de Riego, Instituto de Desarrollo Agropecuario y la Subsecretaría de Agricultura, lo que contraviene el artículo 4° de la ley N° 18.450, ya citada, en cuanto establece que los proyectos deberán ser suscritos por personas previamente calificadas e inscritas en el Registro Público Nacional de Consultores de la Comisión Nacional de Riego.

La repartición precisa en su respuesta que los funcionarios no actúan como consultores en los concursos de la ley, y que la situación descrita por esta Entidad de Control, corresponde a una interpretación de los datos contenidos en el sistema para dichos concursos.

Complementa, indicando que el aludido sistema, en cuanto a su estructura de base de datos, contiene un campo llamado IDUsuario como identificador de consultor, sin opción de utilizar un nuevo campo. Este no mantiene una versión de los perfiles asignados a cada usuario, es decir, si un usuario en su momento actuó como consultor y hoy en día es funcionario de la CNR, al activar su registro y asignarle un rol asociado a sus funciones, aparecerá en la información histórica del concurso como un funcionario actuando como consultor, especificando que lo expuesto anteriormente justifica lo encontrado en los concursos 04-2014 y 07-2012.

16 QA: El aseguramiento de la calidad (conocido también por el anglicismo Quality Assurance) es el conjunto de actividades planificadas y sistemáticas aplicadas en un Sistema de Calidad para que los requisitos de calidad de un producto o servicio sean satisfecho.

Con respecto al concurso N° 31-2015, señala que corresponde a un programa especial de pequeña agricultura sustentado en el inciso tercero del artículo 3° de la ley N° 18.450, que faculta a la repartición a definir las condiciones especiales para la adecuada asignación de recursos. En ese marco, fue el mismo servicio quien determinó que los proyectos fueran ingresados por los mismos funcionarios del Departamento de Fomento al Riego, debiendo utilizar para estos efectos, el mismo campo descrito con anterioridad.

En relación a lo comunicado por la CNR, se constató que para el caso del concurso N° 31-2015, por tratarse de pequeños agricultores y estar regidos por el inciso tercero, del artículo 3° de la citada ley, los hechos expuestos se sustentan bajo la normativa vigente, por lo que la observación se levanta en esta parte.

Asimismo, en lo referente a los hallazgos expuestos que involucran a los concursos N^{os} 04-2014 y 07-2012, se verificó que el registro de consultores y las resoluciones exentas N^{os} 1.159 y 1.854, de 10 de mayo de 2011 y 16 de mayo de 2013, respectivamente, ambas de la aludida comisión, evidencian la inscripción de dichos funcionarios públicos, como consultores, previo a la fecha de postulación, por lo que se levanta lo observado.

27. Deficiencias en la seguridad física del site principal de la CNR.

En el marco de la auditoría, se efectuó una revisión a la sala de servidores de la ODEPA, advirtiéndose una serie de situaciones que infringen lo estipulado en el decreto N° 83, de 2004, las cuales se detallan a continuación:

a) La repartición adolece de un procedimiento formal de control, utilizado para registrar al personal que ingresa a las instalaciones, solicitando su cédula de identidad o pasaporte, incumpliendo lo especificado en la letra e) del artículo 37, relativo a la seguridad física y del ambiente, del nivel avanzado de seguridad del documento electrónico.

b) Los cables de comunicación y de corriente eléctrica no se encuentran separados para mitigar la interferencia del tráfico de datos, contraviniendo lo señalado en el literal precedente.

c) Una de las paredes del perímetro de la sala de servidores no se encuentra construida con concreto o material sólido, lo que conculca lo indicado en la letra e) del artículo antes mencionado.

d) No se dispone de medidas de protección, tales como alarmas en puertas y sensores de movimiento, de forma tal de evitar eventuales robos, pérdidas de información y equipos de procesamiento, infringiendo lo establecido en el artículo 17 del decreto N° 83, de 2004, ya citado.

e) Para los riesgos de incendio y condiciones ambientales, tales como alta temperatura, existencia de humo y humedad, se constató que la sala fiscalizada no posee dispositivos que permitan detectar su existencia, como tampoco

sensores que alerten ante alzas en la temperatura, conforme a lo preceptuado en el aludido artículo 17.

f) Posee un sistema contraincendios que se encontraba deshabilitado al momento de la visita, transgrediendo lo anotado en la letra e) del artículo 37, del ya mencionado decreto.

g) La ubicación del equipamiento de la institución posibilita el riesgo de fugas de agua, contrario a lo estipulado en la letra e) del artículo 37, del precitado decreto.

h) No se cuenta con interruptores generales cercanos a los accesos, vulnerando la misma normativa del literal anterior.

i) El servicio no publicita instrucciones relativas al consumo de alimentos, bebidas y tabaco en las cercanías de sistemas informáticos, según lo previsto en el artículo 18, del referido cuerpo normativo.

j) La institución objeto de esta revisión, no publicita instrucciones relacionadas con la prohibición del uso de medios de grabación, acorde lo mandatado en la letra e), del artículo 37 del aludido decreto.

El servicio auditado en su respuesta consignó que, al momento en que se realizó la visita de esta Contraloría General, se elaboraban trabajos de mejoramiento al interior del datacenter, lo que preliminarmente involucró que el equipo de clima de precisión, ductos y otros dispositivos, pudiesen haber estado fuera de operación temporalmente. Por otra parte, durante dicha inspección, el Departamento de Computación e Informática de ODEPA se trasladaba transitoriamente a otra dependencia.

Para los puntos observados, este Organismo de Control coordinó una nueva visita a la sala en estudio, detectando que las letras a), b), c), d), e), f), g), i) y j) no han sido solucionadas por la repartición, manteniéndose dichas situaciones.

Por otro lado, se subsana lo señalado en el literal h), debido a que el servicio corrigió lo advertido.

28. Deficiencias en la seguridad física del site de contingencia del servicio.

Complementariamente al punto anterior, se efectuó una visita a la sala de servidores secundaria ubicada en las dependencias de la CNR, advirtiéndose situaciones que no se encuentran en conformidad con lo estipulado en el decreto N° 83, de 2004, las cuales se detallan a continuación:

a) La repartición adolece de un procedimiento formal de control, utilizado para registrar al personal que ingresan a las instalaciones, solicitando su cédula de identidad o pasaporte y considerando el propósito de las inspecciones, incumpliendo lo especificado en la letra e) del artículo 37, sobre seguridad física y del ambiente, del nivel avanzado de seguridad del documento electrónico.

b) No todas las paredes del perímetro de la sala de servidores se encuentran construidas de material sólido, lo que conculca lo indicado en la letra e) del artículo 37, ya mencionado.

c) La ubicación del equipamiento de la institución no lo resguarda del riesgo de fugas de agua, según lo estipulado en la normativa ya expresada.

d) El datacenter no dispone de medidas de protección, tales como alarmas en puertas y sensores de movimiento, de forma tal de evitar eventuales robos, pérdidas de información y equipos de procesamiento, infringiendo lo establecido en el artículo 17, del decreto ya citado.

e) En relación con los riesgos de incendio y condiciones ambientales, se constató que el sensor encargado de detectar la existencia de humo dentro de la sala de servidores no se encuentra operativo, lo que vulnera lo anotado en el precitado artículo 17.

f) No se cuenta con interruptores generales cercanos a los accesos, conforme a lo preceptuado en el literal e), del artículo 37, del decreto N° 83.

g) El servicio no publicita instrucciones relativas al consumo de alimentos, bebidas y tabaco en las cercanías de sistemas informáticos, según lo previsto en el artículo 18, del referido cuerpo normativo.

h) La repartición no publicita instrucciones relacionadas con la prohibición del uso de medios de grabación, conforme a lo dispuesto en la letra e) del artículo 37 del precipitado decreto.

i) Los cables de comunicación y de corriente eléctrica no se encuentran separados para mitigar la interferencia del tráfico de datos, contraviniendo lo señalado precedentemente.

j) Las puertas del perímetro de seguridad no poseen las medidas adecuadas contra fuego, acorde a lo manifestado la letra e) del artículo 37 del mencionado decreto.

Al respecto, la repartición en su respuesta indica que es importante consignar que en los meses de febrero y marzo del presente año, la CNR realizó la exploración de alternativas tendientes a mitigar los riesgos asociados a las deficiencias de seguridad física, cuyos trabajos se encuentran planificados de acometer durante el mes de abril de 2016.

Conforme a lo observado, esta Entidad efectuó una nueva inspección a dicha sala, confirmando que las letras c), d), e), g), h), i) y j) no se han corregido por la institución, por lo que se mantienen los citados hechos, en tanto los literales a), b) y f) se subsanan en correspondencia con la solución de las situaciones expuestas.

29. Falta de registro de actividades efectuadas en el Sistema Electrónico Ley 18.450.

Del análisis efectuado a la base de datos destinada al registro de actividades ejecutadas en el sistema, se advirtió que dicha información no cuenta con un campo que individualice al autor de cada operación realizada, como tampoco posee un registro de la hora de inicio y término de los usuarios en el sistema, lo que vulnera lo preceptuado en la letra f), del artículo 37, del decreto N° 83, sobre gestión de las operaciones y comunicaciones.

La repartición en su respuesta señala que, si bien la información que se encuentra en la base de datos no contempla la identificación de las actividades realizadas en este, en ella hay registros que guardan la conexión de los usuarios al sistema y su desconexión, lo que permite hacer un análisis general de las actividades realizadas. Agrega que, dado que contar con dicha información es relevante, esta funcionalidad será incorporada en la nueva versión del Sistema Electrónico Ley 18.450.

Cabe mencionar que lo enunciado por la institución no justifica el hecho observado, dado que la identificación de la conexión y desconexión de usuarios de la base de datos no permite individualizar a los responsables de las acciones críticas ejecutadas dentro del aplicativo en estudio, por lo que se mantiene lo advertido.

30. Omisión en la definición de una fecha de vencimiento para hacer exigible el eventual cobro por concepto de garantía por la prestación de las órdenes de compra ID N^{os} 870-117-CM15 y 870-118-CM15.

En atención a las multas relacionadas con las citadas órdenes de compra, sobre el servicio de mantención y testing UNIBOX, es del caso precisar que el numeral 18 de las bases de licitación, aprobadas por la resolución N° 24, de 14 de enero de 2011, de la Dirección de Compras y Contratación Pública, establece multas por cada día de atraso, respecto del plazo de entrega acordado. Asimismo, la propuesta comercial del proveedor, de 14 de enero de 2015, en su punto 4.1, relativo al Fin del Contrato, indica que la CNR podrá considerar sanciones económicas cuando se dé el "incumplimiento grave de las obligaciones contraídas por Exceed Ltda. Se entenderá por incumplimiento grave la no ejecución o la ejecución parcial en la entrega de productos/servicios o ítems indicados en el presente contrato u orden de compra. En este sentido se considera la responsabilidad que pueda recaer en el personal que disponga la empresa para la realización de alguna tarea encomendada en cualquiera de los servicios contratados o garantías propias del trabajo realizado".

Sobre lo expresado, el administrador de dicho convenio, a través de correo electrónico del 1 de abril de 2016, señaló que la CNR no ha registrado eventos relacionados con la no ejecución total o parcial en la entrega de productos y servicios adquiridos mediante las citadas órdenes de compra, observándose que la entidad omitió definir un vencimiento en el cual se haga exigible la obligación, y que defina la subsecuente aplicación de multas, vulnerando lo previsto

en el artículo 18 del decreto N° 250, de 2004, del Ministerio de Hacienda, ya mencionado.

Al respecto, la CNR en su respuesta indica que las compras por convenio marco, se regulan por las condiciones y obligaciones del referido convenio y de las bases de licitación que la originan, según lo mencionado en el artículo ya referenciado.

Complementa, señalando que las órdenes de compra advertidas se rigen por las cláusulas de multas y garantías de la licitación ID N° 2239-4-LP10 y los acuerdos complementarios que las partes acuerden y/o la propuesta comercial.

Añade que, pese a lo anterior, y dado que desde el año 2016 la entidad está elaborando acuerdos complementarios a las adquisiciones de este tipo, dicho formato se perfeccionará a fin de dejar explícitamente definido el procedimiento de cobro de las multas y garantías.

31. Inexistencia de documentación para ejecutar el examen de las eventuales multas asociadas a las órdenes de compra N^{os} 870-965-CM14 y 870-981-CM14.

Respecto al análisis del servicio de suministro del Software Red Hat JBOSS, proporcionado por la empresa Computación e Ingeniería S.A., el numeral 18 de las bases de licitación, aprobadas por la resolución N° 24, de 14 de enero de 2011, de la Dirección de Compras y Contratación Pública, especifica que "Las multas por atraso en la entrega se aplicarán por cada día hábil de atraso, y se calcularán como un 1,5% del valor del ítem o producto solicitado y aplicable a las cantidades que se entreguen atrasadas, por cada día hábil de atraso, respecto del plazo de entrega acordado".

En relación con lo anterior, el Administrador del Sistema Electrónico Ley 18.450, confirmó por correo de 1 de abril de 2016, que no existe documentación que especifique una fecha de entrega del producto, imposibilitando determinar la existencia de sanciones relativas a la adquisición. Sin embargo, es del caso precisar que de acuerdo al reporte web del proveedor, este indica que los servicios de suscripción fueron iniciados el 15 de marzo de 2015, observándose que la entidad omitió definir un vencimiento en que se haga exigible la obligación, contraviniendo lo establecido en el artículo 18, del decreto N° 250, de 2004, antes citado.

Para el hecho descrito, la repartición comunica en su respuesta que, del mismo modo que en la observación anterior, esta se subsanará, perfeccionando los acuerdos complementarios donde se establezca el o los plazos de vencimiento de los hitos de la compra para ser aplicables las multas.

Conforme a las respuestas descritas por el servicio en los numerales 30 y 31, esta Contraloría General mantiene los hechos observados puesto que la repartición confirma la omisión del establecimiento de una fecha de entrega de las aludidas adquisiciones, lo cual provocó la imposibilidad de

aplicar un eventual cobro por concepto de garantías o multas en caso de retrasos, lo cual debió ser recogido en el correspondiente acuerdo complementario al convenio marco respectivo.

III. EXAMEN DE CUENTAS

En esta auditoría se comprobó el cumplimiento de las disposiciones legales y reglamentarias que rigen los gastos examinados, la veracidad y fidelidad de las cuentas, la autenticidad y pertinencia de la documentación respectiva, y que el gasto fuese autorizado por funcionario competente, en relación con los convenios incluidos en la muestra de la presente auditoría, detallados en el Anexo N° 9, al tenor de lo dispuesto en los artículos 95 y siguientes de la ley N° 10.336, antes mencionada.

En relación con la materia, se verificó que, en general, los egresos relacionados con los bienes y servicios de la muestra revisada se ajustan a la normativa legal y reglamentaria vigente, además de contar con la documentación de respaldo correspondiente, sin observaciones que señalar.

Asimismo, se verificó, respecto de los bienes adquiridos, que estos se encuentran debidamente registrados en los sistemas contable y administrativo del servicio. De igual manera, se constataron los procedimientos de recepción y entrega de los mismos a los funcionarios responsables de su custodia, lo cual no generó situaciones que representar.

CONCLUSIONES

Atendidas las consideraciones expuestas durante el desarrollo del presente trabajo, la Comisión Nacional de Riego ha aportado antecedentes e iniciado acciones que han permitido salvar parte de las objeciones formuladas en el preinforme de observaciones N° 305, de 2016, de esta Contraloría General.

En efecto, las observaciones planteadas en el capítulo II, Examen de la Materia Auditada, numerales 27, Deficiencias en la seguridad física del site principal de la CNR, letra h); y 28, Deficiencias en la seguridad física del site de contingencia del servicio, letras a), b) y f), se subsanan, conforme a los antecedentes y argumentos aportados por el servicio.

Seguidamente, los hallazgos expuestos en el capítulo I, Aspectos de Control Interno, numerales 1, Ausencia de seguimiento de las observaciones emanadas de la auditoría externa realizada por la empresa Decalink Ltda., y 2, Falta de estipulación contractual para la prestación relativa a enlace de datos MPLS; y en el capítulo II, Examen de la Materia Auditada, numerales 10, Uso de software no licenciado, y 26, Funcionarios asignados como consultores a concursos, se levantan, en conformidad a la documentación suministrada por el servicio.

En lo que concierne al mencionado capítulo II, numerales 11, Uso de software descontinuado y sin soporte, y 14, Carencia de un registro de intentos de acceso fallidos al Sistema Electrónico Ley 18.450, este Ente Contralor recomienda a esta institución tomar medidas respecto a ambas situaciones, a fin de mejorar sus controles internos.

Para lo descrito en el mismo capítulo, numerales 21, Cierre de incidencia sin medida adoptada (AC)[17]; 22, Modificaciones en las variables de postulación posterior a la fecha de apertura (AC)[18]; 25, Falta de eficacia al contratar productos Red Hat para la creación de la nueva versión del Sistema Electrónico Ley 18.450 (C)[19]; 30, Omisión en la definición de una fecha de vencimiento para hacer exigible el eventual cobro por concepto de garantía por la prestación de las órdenes de compra ID N^{os} 870-117-CM15 y 870-118-CM15 (C)[20] y 31, Inexistencia de documentación para ejecutar el examen de las eventuales multas asociadas a las órdenes de compra ID N^{os} 870-965-CM14 y 870-981-CM14 (C)[21]; la CNR deberá instruir un sumario administrativo a fin de establecer posibles responsabilidades para los hechos descritos, remitiendo a este Organismo de Control, en el término de 15 días hábiles contado desde la recepción del presente informe, el acto administrativo mediante el cual se disponga tal proceso y se designe al fiscal.

Sobre aquellas observaciones que se mantienen, se deberán adoptar medidas con el objeto de dar estricto cumplimiento a las normas legales y reglamentarias pertinentes, entre las cuales se estima necesario considerar, a lo menos, las siguientes:

1. Con respecto al capítulo II, Examen de la Materia Auditada, numeral 1, Falta de mecanismos de revisión periódica a la integridad de la información (C)[22], la CNR deberá desarrollar y sancionar mecanismos de revisión periódica a la integridad de la información del Sistema Electrónico Ley 18.450, suministrando un informe de avance a esta Entidad de Control en el término de 60 días hábiles contados desde la recepción del presente informe final.

Relativo a lo expuesto en el numeral 2, Omisión de pruebas al plan de continuidad del negocio (C)[23], el servicio deberá informar en el mismo plazo el resultado de al menos una prueba realizada al plan de continuidad del negocio, en el mismo plazo ya anotado, en donde se identifique claramente que los riesgos expuestos en el plan fueron analizados y el resultado final.

A su turno en el numeral 3, Carencia de un programa de actualización al plan de contingencia (AC[24]), la entidad deberá actualizar el aludido plan y agregar un control de cambios al documento, identificando la fecha y

17 Observación Altamente Compleja: Falencias de seguridad de sistemas.
18 Observación Altamente Compleja: Falencias de seguridad de sistemas.
19 Observación Compleja: Existencia de actos, que causan detrimento fiscal.
20 Observación Compleja: Incumplimiento de normativa relacionada con el proceso de compras.
21 Observación Compleja: Incumplimiento de normativa relacionada con el proceso de compras.
22 Observación Compleja: Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres de 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.
23 Observación Compleja: Inexistencia de planes de contingencia.
24 Observación Altamente Compleja: Inexistencia de planes de contingencia.

responsable de cada una de sus versiones. Adicionalmente, una vez culminado el proceso de actualización, este documento tendrá que ser formalizado y suministrado a esta Entidad Fiscalizadora, informando su estado de avance en un plazo máximo de 60 días hábiles, contados desde la recepción del presente informe.

Para lo manifestado en el numeral 4, Falta de controles físicos considerados en el procedimiento de control de acceso a la sala de servidores (C[25]), la Comisión Nacional de Riego deberá actualizar y formalizar el procedimientos de control de acceso al datacenter, a fin de considerar los hechos expuestos en la observación, junto con establecer las medidas correctivas atingentes al hallazgo, debiendo informar de sus avances a este Organismo de Control, en un plazo de 60 días hábiles, contados desde la recepción del presente informe final.

De lo expuesto en el numeral 5, Debilidades en el control de acceso a redes externas (C[26]), el servicio deberá suministrar en el plazo antedicho, documentación que evidencie las medidas adoptadas para que a nivel de firewall, se restrinja la conexión a sitios y protocolos que permitan la descarga de contenido no confiable en internet, tales como mega.nz y BitTorrent[27]. Esto debe ser aplicado tanto para equipos externos como internos, conectados a internet, mediante el uso de la red institucional.

Además, en lo que compete al numeral 6, Ausencia de estrategias de recuperación ante desastres (AC[28]), la CNR deberá incorporar los distintos planes de recuperación atingentes a cada uno de los sistemas críticos del plan de contingencia, informando su estado de avance en un plazo de 60 días hábiles, contados desde la recepción del presente informe.

Con respecto al numeral 7, Carencia de una política que instruya sobre el uso del correo electrónico institucional (C[29]), la CNR tendrá que desarrollar y sancionar una política que imparta instrucciones sobre aquello, acreditando la medida en el mismo plazo ya mencionado.

Relativo al numeral 8, Falta de un proceso formal de inducción a las medidas de seguridad TI adoptadas por la institución (C[30]), la repartición deberá elaborar y formalizar de manera documental el citado proceso de capacitación, suministrándolo a este Organismo de Control en el plazo de 60 días hábiles, contados desde la recepción de este informe final.

---

25 Observación Compleja: Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres de 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.
26 Observación Compleja: Falta de políticas de resguardo de la información o que estas no se encuentren formalizadas.
27 BitTorrent: Protocolo diseñado para el intercambio de archivos en internet, destacado por ser uno de los más comunes para la transferencia de contenido pesado.
28 Observación Altamente Compleja: Inexistencia de planes de contingencia.
29 Observación Compleja: Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres de 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.
30 Observación Compleja: Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.

Sobre lo consignado en el numeral 9, Falta de seguridad en el sitio externo de almacenamiento (C)[31], la institución deberá efectuar las evaluaciones técnicas correspondientes a la viabilidad de la implementación de las acciones correctivas, informado su estado de avance en el plazo ya anotado.

En lo correspondiente al numeral 12, Autentificación débil en el Sistema Electrónico Ley 18.450 (AC)[32], la Comisión Nacional de Riego deberá actualizar todas las contraseñas administradas en el sistema, comunicando las medidas adoptadas y acompañando los antecedentes de respaldo respectivos, en un plazo máximo de 60 días hábiles, contados desde la recepción de este informe.

De lo expuesto en el numeral 13, Falta de revisión de los permisos de acceso (AC)[33], la entidad deberá llevar cabo un proceso de revisión de usuarios desvinculados en cada uno de los sistemas críticos institucionales, como también, actualizar y posteriormente formalizar el procedimiento denominado Gestión de Acceso a Redes Locales y Servicio Mensajería Electrónica, debiendo informar del estado de avance, en el mismo plazo ya anotado.

Con respecto al numeral 15, Deficiencia en el control y gestión del inventario TI (C)[34], la CNR tendrá que realizar una revisión del inventario de los servidores físicos, en conjunto con el área responsable de activos del servicio, constatando el correcto registro de cada activo, identificando como mínimo, su número de inventario y de serie, modelo, ubicación física y características técnicas, lo cual deberá acreditar en el mismo plazo ya referido.

Para lo manifestado en el numeral 16, Falencias en el control de acceso al Sistema Electrónico Ley 18.450 (AC)[35], considerando que actualmente existen concursos en ejecución, la repartición deberá analizar y solucionar las vulnerabilidades asociadas a la manipulación de parámetros en los enlaces del aplicativo web, informando el estado de avance de esta evaluación y posterior implementación, en un plazo máximo de 60 días hábiles, contados desde la recepción de este reporte.

A su turno, en lo que compete al numeral 17, Ausencia de controles que restrinjan el cambio de perfilamiento (AC)[36], la Comisión Nacional de Riego deberá evaluar y corregir lo advertido, informando el estado de avance en lo relativo al análisis e implementación de medidas correctivas en el sistema, en un plazo máximo de 60 días hábiles, contados desde la fecha de recepción del presente informe.

---

31 Observación Compleja: Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.
32 Observación Altamente Compleja: Falencias de seguridad de sistemas.
33 Observación Altamente Compleja: Falencias de seguridad de sistemas.
34 Observación Compleja: Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres de 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.
35 Observación Altamente Compleja: Falencias de seguridad de sistemas.
36 Observación Altamente Compleja: Falencias de seguridad de sistemas.

Relativo a lo expresado en el numeral 18, Falla de controles de acceso a información confidencial de proyectos (AC)[37], la CNR deberá tomar medidas tendientes a solucionar las brechas de seguridad detectadas, a fin de resguardar la confidencialidad de la información, evaluando el estado actual del sistema, informando de los avances dentro del plazo de 60 días hábiles, contados en la forma ya anotada.

En lo correspondiente al numeral 19, Deficiencia de controles de acceso a la base de datos (AC)[38], la CNR deberá establecer un procedimiento para llevar un registro de los cambios realizados y aprobados por la jefatura del Departamento de Fomento al Riego, informando del avance en el mismo plazo ya anotado.

Considerando lo consignado en el numeral 20, Hallazgo de vulnerabilidad sin subsanación (AC)[39], la Comisión Nacional de Riego deberá realizar la reparación del software en estudio, respecto a las debilidades indicadas en los correos electrónicos del 10 y 23 de diciembre de 2013, informándose a este Ente de Control en un periodo de 60 días hábiles, contados desde la recepción del presente informe.

Relativo a lo expuesto al ya citado numeral 21, Cierre de incidencia sin medida adoptada, y sin perjuicio del sumario administrativo que debe instruir, el servicio deberá analizar la corrección de la incidencia descrita en el ticket N° 318 de 2012, informando su estado de avance, en el plazo de 60 días hábiles, contados desde la recepción del presente informe final.

Para lo indicado en el numeral 22, Modificaciones en las variables de postulación posterior a la fecha de apertura, sin perjuicio del sumario administrativo que debe instruirse, la entidad deberá desarrollar controles de carácter sistémico para evitar la alteración de las variables de postulación, de modo de evitar que tales incidentes se repitan, lo cual será verificado en futuras fiscalizaciones.

Sobre lo expuesto en el numeral 23, Vulnerabilidades de seguridades informadas en la auditoría externa en el año 2014 y no subsanadas (AC)[40], la CNR deberá definir y sancionar un procedimiento de atención de incidencias que registre las acciones tomadas por el encargado de seguridad. Asimismo, deberá regularizar todas las fallas de seguridad expuestas en el Anexo N° 7, remitiendo a esta Contraloría General, en ambos casos, el informe de avance en el mismo plazo ya anotado.

En lo correspondiente al numeral 24, Sistema permite consultar datos de los postulantes a concursos a través del formulario de búsqueda (AC)[41], la institución auditada deberá levantar un análisis de las causales de

37 Observación Altamente Compleja: Falencias de seguridad de sistemas.
38 Observación Altamente Compleja: Falencias de seguridad de sistemas.
39 Observación Altamente Compleja: Falencias de seguridad de sistemas.
40 Observación Altamente Compleja: Falencias de seguridad de sistemas.
41 Observación Altamente Compleja: Falencias de seguridad de sistemas.

la falla de seguridad, junto con informar el estado de avance de las medidas correctivas aplicadas, en un período de 60 días hábiles, contados desde la recepción del presente informe final.

Para el numeral 25, Falta de eficacia al contratar productos Red Hat para la creación de la nueva versión del Sistema Electrónico Ley 18.450, adicionalmente al proceso disciplinario ordenado instruir, la CNR deberá informar el estado de avance del nuevo aplicativo, al que se refiere en su respuesta, en el término de 60 días hábiles.

En lo que toca al numeral 27, Deficiencias en la seguridad física del site principal de la CNR (C)[42], el servicio deberá efectuar las siguientes acciones:

- Desarrollar y sancionar un procedimiento formal de control de acceso, para registrar al personal que ingresa a las instalaciones, solicitando su cédula de identidad o pasaporte.

- Separar los cables de comunicación y de corriente eléctrica, a fin de mitigar la interferencia del tráfico de datos.

- Disponer un perímetro para la sala de servidores, de concreto o material sólido.

- Incorporar en dicho lugar, alarmas en puertas y sensores de movimiento, de forma tal de evitar eventuales robos, pérdidas de información y equipos de procesamiento.

- Instalar dispositivos que permitan detectar la existencia de humo, humedad, y alzas de temperatura.

- Disponer un sistema contra incendios del tipo eléctrico.

- Certificar la mitigación del riesgo de fugas de agua dentro de la ubicación del equipamiento de la institución, por una entidad del rubro.

- Señalizar instrucciones relativas al consumo de alimentos, bebidas, tabaco y medios de grabación, en las cercanías de los dispositivos informáticos.

Para todas ellas deberá informar su estado de avance, en un plazo de 60 días hábiles, contados desde la recepción del presente informe final.

Luego, para lo manifestado en el numeral 28, deficiencias en la seguridad física del site de contingencia del servicio (C[43]), a la repartición le corresponderá:

---

42 Observación Compleja: Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres de 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.
43 Observación Compleja: Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres de 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.

- Disponer un perímetro para la sala de servidores, de concreto o material sólido.
- Separar los cables de comunicación y de corriente eléctrica, a fin de mitigar la interferencia del tráfico de datos.
- Incorporar en dicho lugar, alarmas en puertas y sensores de movimiento, de forma tal de evitar eventuales robos, pérdidas de información y equipos de procesamiento.
- Colocar un sensor detector de humo.
- Certificar la mitigación del riesgo de fugas de agua dentro de la ubicación del equipamiento de la institución, por una entidad del rubro.
- Señalizar instrucciones relativas al consumo de alimentos, bebidas, tabaco y medios de grabación, en las cercanías de los dispositivos informáticos.
- Instalar en el site mencionado, una puerta contra fuego.

El estado de avance de tales medidas deberá ser informado a esta Entidad de Control en el plazo de 60 días hábiles, contados desde la recepción del presente informe.

Con respecto al numeral 29, falta de registro de actividades efectuadas en el Sistema Electrónico Ley 18.450 (C)[44], la CNR tendrá que incorporar al software en cuestión, la funcionalidad de registrar los nombres de los usuarios que realicen transacciones sensibles dentro del aplicativo, detallando fecha y hora, acción realizada y terminal utilizado, acreditando la medida en el mismo plazo ya anotado.

Para los numerales 30, Omisión en la definición de una fecha de vencimiento para hacer exigible el eventual cobro por concepto de garantía por la prestación de las órdenes de compra ID N^{os} 870-117-CM15 y 870-118-CM15; y 31, Inexistencia de documentación para ejecutar el examen de las eventuales multas asociadas a las órdenes de compra ID N^{os} 870-965-CM14 y 870-981-CM14, en lo sucesivo, el servicio deberá definir e incorporar las fechas asociadas a la provisión de bienes o servicios, en los convenios que establezca con los proveedores, lo que será validado en futuras auditorías.

Finalmente, para aquellas observaciones que se mantienen, se deberá remitir el "Informe de Estado de Observaciones" de acuerdo al formato adjunto en Anexo N° 12, en un plazo máximo de 60 días hábiles, o en el que específicamente se haya señalado, contado desde la recepción del presente informe, comunicando las medidas adoptadas y acompañando los antecedentes de respaldo respectivos.

---

44 Observación Compleja: Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres de 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.

Transcríbase el presente informe al señor Ministro de Agricultura de la referida cartera de Estado, a la Secretaria Ejecutiva y al coordinador de la Unidad de Auditoría Interna, ambos de la Comisión Nacional de Riego; a las Unidades Técnica de Control Externo y de Seguimiento, ambas de la División de Auditoría Administrativa; a la Unidad de Seguimiento de Fiscalía, las tres últimas de esta Contraloría General; y a don [redacted], autor de la denuncia N° W001133, de 2015.

Saludos atentamente a Ud.,

JEAN PAUL THIBAUT VERDUGO
Jefe Unidad de Auditoría de Sistemas
División de Auditoría Administrativa

ANEXO N° 1

Listado de usuarios vigentes asociados a personal desvinculado.

N° de usuario	Rut	Nombre	
705	[redacted]		
770			
800			
8865			
21576			
23757			

Fuente: Elaborado por la Contraloría General de acuerdo a los antecedentes proporcionados por la Comisión Nacional de Riego, a través del oficio ORD. N° 228, de 22 de enero de 2016 y la información almacenada en la base de datos del Sistema Electrónico Ley 18.450.

ANEXO N° 2

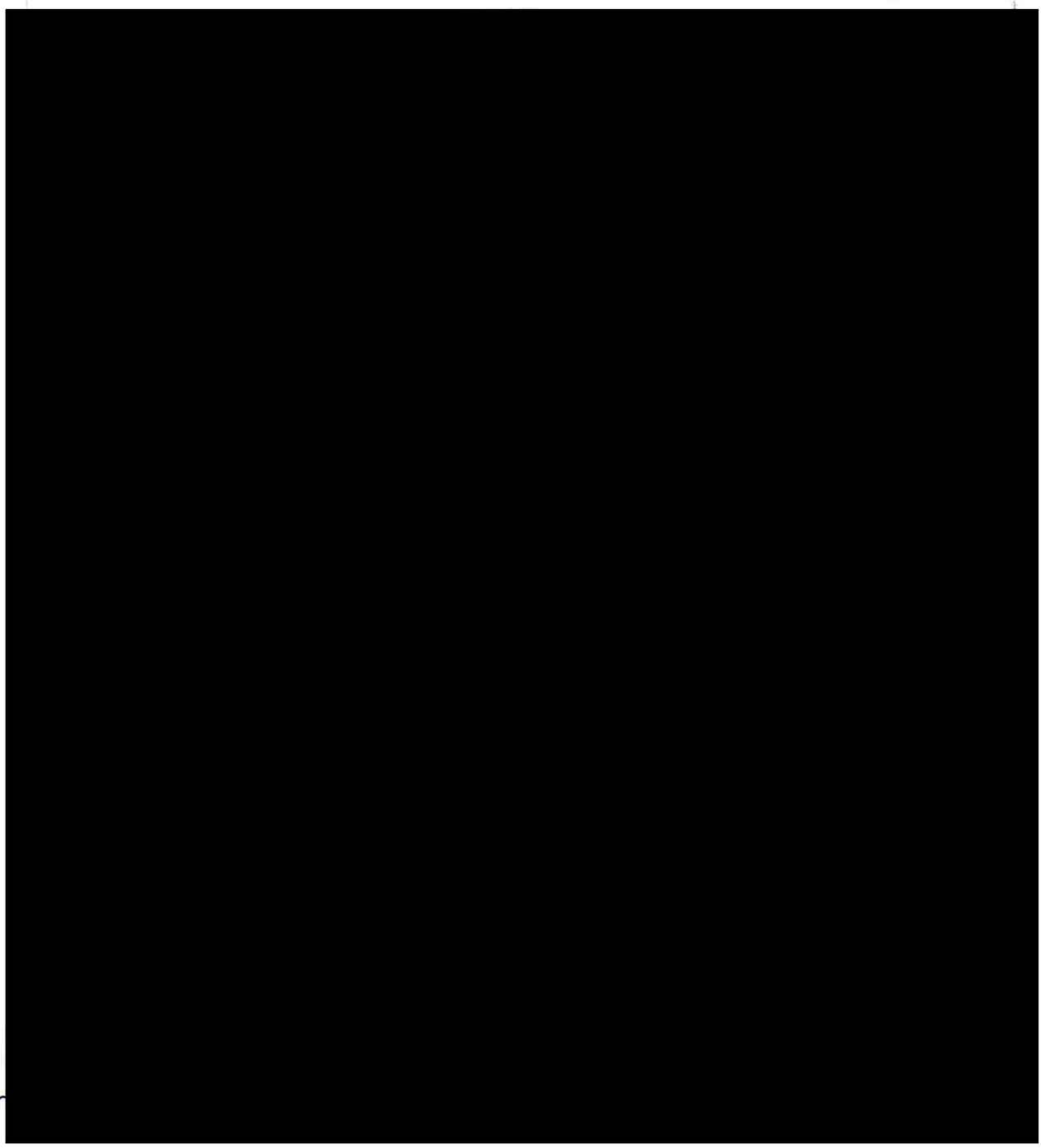
Equipos de TI no encontrados debido a la inconsistencia de números de inventario en el hardware de los equipos analizados.

Código Activo	Proveedor
000290613001	DELL COMPUTER DE CHILE LIMITADA
000290613002	DELL COMPUTER DE CHILE LIMITADA
000290613003	DELL COMPUTER DE CHILE LIMITADA
000290613004	DELL COMPUTER DE CHILE LIMITADA
000290613005	DELL COMPUTER DE CHILE LIMITADA
000290613006	DELL COMPUTER DE CHILE LIMITADA
000290613007	DELL COMPUTER DE CHILE LIMITADA
000290613008	DELL COMPUTER DE CHILE LIMITADA
000290613009	DELL COMPUTER DE CHILE LIMITADA
000290613010	DELL COMPUTER DE CHILE LIMITADA
000290613011	DELL COMPUTER DE CHILE LIMITADA
000290613012	DELL COMPUTER DE CHILE LIMITADA
000290613013	DELL COMPUTER DE CHILE LIMITADA
000290613014	DELL COMPUTER DE CHILE LIMITADA
000290613015	DELL COMPUTER DE CHILE LIMITADA
000290613016	DELL COMPUTER DE CHILE LIMITADA
000290613017	DELL COMPUTER DE CHILE LIMITADA
000290613018	DELL COMPUTER DE CHILE LIMITADA
000290613019	DELL COMPUTER DE CHILE LIMITADA
000290613020	DELL COMPUTER DE CHILE LIMITADA
000290613021	DELL COMPUTER DE CHILE LIMITADA
000290613022	SOC. PARDOW GUZMAN & WEBER LIMITADA
000290613023	TRANSACTION LINE CHILE S.A.
000290613024	TRANSACTION LINE CHILE S.A.

Fuente: Elaborado por la Contraloría General de acuerdo a los antecedentes proporcionados por la Comisión Nacional de Riego, a través del correo electrónico del 5 de febrero de 2016, de parte del Coordinador de la Unidad de Soporte Informático.

ANEXO N° 3

Cambio de parámetro en la URL que permite acceder al sistema sin credenciales de autentificación.



ANEXO N° 4

Sistema permite acceder sin credenciales al perfil de administrador (ejemplo utilizando Google Chrome).

1)

2)

ANEXO N° 5

Comparación de las simulaciones de puntajes considerando los valores asignados a las variables más recientes, antes de la fecha de apertura y los resultados oficiales obtenidos, infringiendo la normativa de las bases concursales.

Código Concurso	Código del Proyecto	Resultado de la Corrida Puntaje Oficial del Concurso (Como fue)	Resultado de la Corrida Puntaje Aplicando la Normativa (Como debió haber sido)
19-2014	16-2011-15-021	Seleccionado	No Seleccionado
20-2014	20-2014-07-003	No Seleccionado	Seleccionado
20-2014	20-2014-04-018	No Seleccionado	Seleccionado
20-2014	20-2014-07-030	No Seleccionado	Seleccionado
20-2014	20-2014-07-029	No Seleccionado	Seleccionado
20-2014	20-2014-04-015	No Seleccionado	Seleccionado
20-2014	20-2014-07-025	No Seleccionado	Seleccionado
20-2014	20-2014-06-008	No Seleccionado	Seleccionado
20-2014	20-2014-04-014	No Seleccionado	Seleccionado
20-2014	20-2014-04-013	No Seleccionado	Seleccionado
20-2014	20-2014-04-016	No Seleccionado	Seleccionado
20-2014	01-2014-08-004	No Seleccionado	Seleccionado
20-2014	19-2013-07-023	No Seleccionado	Seleccionado
20-2014	20-2014-07-051	No Seleccionado	Seleccionado
20-2014	09-2014-08-002	No Seleccionado	Seleccionado
20-2014	20-2014-07-024	No Seleccionado	Seleccionado
20-2014	13-2014-15-003	No Seleccionado	Seleccionado
20-2014	13-2014-15-002	No Seleccionado	Seleccionado
20-2014	20-2014-07-011	No Seleccionado	Seleccionado
22-2014	22-2014-04-041	No Seleccionado	Seleccionado
22-2014	22-2014-07-025	No Seleccionado	Seleccionado
22-2014	23-2013-04-006	No Seleccionado	Seleccionado
22-2014	08-2013-07-008	No Seleccionado	Seleccionado
22-2014	09-2014-07-013	No Seleccionado	Seleccionado
22-2014	09-2014-04-020	No Seleccionado	Seleccionado
22-2014	22-2014-04-016	No Seleccionado	Seleccionado
22-2014	22-2014-04-018	No Seleccionado	Seleccionado
22-2014	22-2014-04-009	No Seleccionado	Seleccionado
22-2014	09-2014-07-008	No Seleccionado	Seleccionado
22-2014	09-2014-07-009	No Seleccionado	Seleccionado
22-2014	09-2014-08-001	No Seleccionado	Seleccionado
22-2014	09-2014-08-002	No Seleccionado	Seleccionado
23-2014	23-2014-07-181	No Seleccionado	Seleccionado
23-2014	23-2014-07-050	No Seleccionado	Seleccionado
23-2014	23-2014-07-045	No Seleccionado	Seleccionado
23-2014	23-2014-08-044	No Seleccionado	Seleccionado
23-2014	23-2014-07-096	No Seleccionado	Seleccionado
23-2014	23-2014-07-191	No Seleccionado	Seleccionado
23-2014	23-2014-07-113	No Seleccionado	Seleccionado
23-2014	23-2014-08-069	No Seleccionado	Seleccionado
23-2014	23-2014-07-218	No Seleccionado	Seleccionado
23-2014	23-2014-07-175	No Seleccionado	Seleccionado
23-2014	23-2014-07-164	No Seleccionado	Seleccionado
23-2014	23-2014-07-071	No Seleccionado	Seleccionado
23-2014	23-2014-07-064	No Seleccionado	Seleccionado
23-2014	23-2014-07-151	No Seleccionado	Seleccionado
23-2014	23-2014-07-067	No Seleccionado	Seleccionado
23-2014	23-2014-07-057	No Seleccionado	Seleccionado
23-2014	23-2014-07-124	No Seleccionado	Seleccionado
23-2014	23-2014-07-080	No Seleccionado	Seleccionado
23-2014	23-2014-07-025	No Seleccionado	Seleccionado

Código Concurso	Código del Proyecto	Resultado de la Corrida Puntaje Oficial del Concurso (Como fue)	Resultado de la Corrida Puntaje Aplicando la Normativa (Como debió haber sido)
23-2014	24-2013-07-005	No Seleccionado	Seleccionado
23-2014	23-2014-07-110	No Seleccionado	Seleccionado
23-2014	21-2013-08-081	No Seleccionado	Seleccionado
23-2014	23-2014-07-094	No Seleccionado	Seleccionado
23-2014	23-2014-07-200	No Seleccionado	Seleccionado
23-2014	23-2014-07-116	No Seleccionado	Seleccionado
23-2014	23-2014-07-208	No Seleccionado	Seleccionado
23-2014	23-2014-07-162	No Seleccionado	Seleccionado
23-2014	23-2014-07-059	No Seleccionado	Seleccionado
23-2014	23-2014-07-171	No Seleccionado	Seleccionado
23-2014	23-2014-07-201	No Seleccionado	Seleccionado
23-2014	23-2014-08-038	No Seleccionado	Seleccionado
23-2014	23-2014-07-100	No Seleccionado	Seleccionado
23-2014	23-2014-07-153	No Seleccionado	Seleccionado
23-2014	23-2014-07-134	No Seleccionado	Seleccionado
23-2014	23-2014-08-068	No Seleccionado	Seleccionado
23-2014	23-2014-07-107	No Seleccionado	Seleccionado
23-2014	23-2014-07-131	No Seleccionado	Seleccionado
23-2014	23-2014-07-007	No Seleccionado	Seleccionado
23-2014	23-2014-07-160	No Seleccionado	Seleccionado
23-2014	23-2014-07-136	No Seleccionado	Seleccionado
23-2014	23-2014-07-063	No Seleccionado	Seleccionado
23-2014	23-2014-07-006	No Seleccionado	Seleccionado
23-2014	23-2014-07-189	No Seleccionado	Seleccionado
23-2014	23-2014-08-060	No Seleccionado	Seleccionado
23-2014	23-2014-07-035	No Seleccionado	Seleccionado
23-2014	23-2014-07-104	No Seleccionado	Seleccionado
23-2014	23-2014-07-079	No Seleccionado	Seleccionado
23-2014	23-2014-07-195	No Seleccionado	Seleccionado
23-2014	23-2014-07-167	No Seleccionado	Seleccionado
23-2014	21-2013-08-061	No Seleccionado	Seleccionado
23-2014	24-2013-07-027	No Seleccionado	Seleccionado
23-2014	23-2014-07-149	No Seleccionado	Seleccionado
23-2014	21-2012-08-079	No Seleccionado	Seleccionado
23-2014	23-2014-07-157	No Seleccionado	Seleccionado
23-2014	23-2014-07-205	No Seleccionado	Seleccionado
23-2014	23-2014-08-001	No Seleccionado	Seleccionado
23-2014	24-2013-07-086	No Seleccionado	Seleccionado
23-2014	23-2014-07-147	No Seleccionado	Seleccionado
23-2014	23-2014-07-005	No Seleccionado	Seleccionado
23-2014	24-2013-07-075	No Seleccionado	Seleccionado
23-2014	23-2014-07-108	No Seleccionado	Seleccionado
23-2014	23-2014-07-184	No Seleccionado	Seleccionado
23-2014	23-2014-07-163	No Seleccionado	Seleccionado
23-2014	23-2014-07-027	No Seleccionado	Seleccionado
23-2014	07-2013-08-073	No Seleccionado	Seleccionado
23-2014	23-2014-07-019	No Seleccionado	Seleccionado
23-2014	23-2014-07-202	No Seleccionado	Seleccionado
23-2014	23-2014-08-066	No Seleccionado	Seleccionado
23-2014	23-2014-07-090	No Seleccionado	Seleccionado
23-2014	23-2014-07-207	No Seleccionado	Seleccionado
23-2014	23-2014-07-180	No Seleccionado	Seleccionado
23-2014	23-2014-08-077	No Seleccionado	Seleccionado
23-2014	23-2014-07-083	No Seleccionado	Seleccionado
23-2014	23-2014-07-128	No Seleccionado	Seleccionado
23-2014	23-2014-07-187	No Seleccionado	Seleccionado
23-2014	23-2014-08-019	No Seleccionado	Seleccionado
23-2014	23-2014-07-188	No Seleccionado	Seleccionado

Código Concurso	Código del Proyecto	Resultado de la Corrida Puntaje Oficial del Concurso (Como fue)	Resultado de la Corrida Puntaje Aplicando la Normativa (Como debió haber sido)
23-2014	23-2014-07-129	No Seleccionado	Seleccionado
23-2014	23-2014-07-130	No Seleccionado	Seleccionado
23-2014	23-2014-07-158	No Seleccionado	Seleccionado
23-2014	23-2014-08-067	No Seleccionado	Seleccionado
23-2014	23-2014-07-010	No Seleccionado	Seleccionado
23-2014	23-2014-07-013	No Seleccionado	Seleccionado
23-2014	23-2014-07-185	No Seleccionado	Seleccionado
23-2014	23-2014-07-183	No Seleccionado	Seleccionado
23-2014	23-2014-08-083	No Seleccionado	Seleccionado
23-2014	23-2014-07-177	No Seleccionado	Seleccionado
23-2014	23-2014-07-193	No Seleccionado	Seleccionado
23-2014	23-2014-07-211	No Seleccionado	Seleccionado
23-2014	23-2014-07-194	No Seleccionado	Seleccionado
23-2014	23-2014-07-212	No Seleccionado	Seleccionado
23-2014	23-2014-07-179	No Seleccionado	Seleccionado
23-2014	23-2014-07-052	No Seleccionado	Seleccionado
23-2014	23-2014-07-032	No Seleccionado	Seleccionado
23-2014	23-2014-07-186	No Seleccionado	Seleccionado
23-2014	23-2014-07-068	No Seleccionado	Seleccionado
23-2014	23-2014-07-154	No Seleccionado	Seleccionado
23-2014	23-2014-07-011	No Seleccionado	Seleccionado
23-2014	23-2014-07-066	No Seleccionado	Seleccionado
23-2014	23-2014-07-159	No Seleccionado	Seleccionado
23-2014	23-2014-07-004	No Seleccionado	Seleccionado
23-2014	23-2014-08-059	No Seleccionado	Seleccionado
23-2014	23-2014-07-058	No Seleccionado	Seleccionado
23-2014	23-2014-08-058	No Seleccionado	Seleccionado
23-2014	23-2014-07-125	No Seleccionado	Seleccionado
23-2014	23-2014-07-169	No Seleccionado	Seleccionado
23-2014	23-2014-07-008	No Seleccionado	Seleccionado
23-2014	23-2014-07-077	No Seleccionado	Seleccionado
23-2014	23-2014-07-161	No Seleccionado	Seleccionado
23-2014	23-2014-07-061	No Seleccionado	Seleccionado
23-2014	23-2014-07-053	No Seleccionado	Seleccionado
23-2014	23-2014-07-085	No Seleccionado	Seleccionado
23-2014	23-2014-08-047	No Seleccionado	Seleccionado
23-2014	23-2014-07-060	No Seleccionado	Seleccionado
23-2014	23-2014-07-204	No Seleccionado	Seleccionado
23-2014	23-2014-07-172	No Seleccionado	Seleccionado
23-2014	23-2014-07-196	No Seleccionado	Seleccionado
23-2014	23-2014-07-009	No Seleccionado	Seleccionado
23-2014	23-2014-07-036	No Seleccionado	Seleccionado
23-2014	23-2014-07-140	No Seleccionado	Seleccionado
23-2014	23-2014-07-074	No Seleccionado	Seleccionado
23-2014	23-2014-07-065	No Seleccionado	Seleccionado
23-2014	23-2014-07-082	No Seleccionado	Seleccionado
23-2014	23-2014-07-148	No Seleccionado	Seleccionado
23-2014	23-2014-07-084	No Seleccionado	Seleccionado
23-2014	07-2014-08-068	No Seleccionado	Seleccionado
23-2014	02-2014-07-010	No Seleccionado	Seleccionado
23-2014	21-2013-08-053	No Seleccionado	Seleccionado
23-2014	23-2014-07-012	No Seleccionado	Seleccionado
23-2014	23-2014-07-142	No Seleccionado	Seleccionado
23-2014	21-2012-08-059	No Seleccionado	Seleccionado
23-2014	07-2014-08-019	No Seleccionado	Seleccionado
23-2014	07-2014-08-032	No Seleccionado	Seleccionado
23-2014	18-2011-08-044	No Seleccionado	Seleccionado
23-2014	02-2014-07-019	No Seleccionado	Seleccionado

Código Concurso	Código del Proyecto	Resultado de la Corrida Puntaje Oficial del Concurso (Como fue)	Resultado de la Corrida Puntaje Aplicando la Normativa (Como debió haber sido)
23-2014	02-2014-07-002	No Seleccionado	Seleccionado
23-2014	21-2012-08-055	No Seleccionado	Seleccionado
23-2014	02-2014-07-025	No Seleccionado	Seleccionado
23-2014	15-2013-07-066	No Seleccionado	Seleccionado
23-2014	21-2013-08-069	No Seleccionado	Seleccionado
23-2014	06-2012-08-033	No Seleccionado	Seleccionado
23-2014	23-2014-07-055	No Seleccionado	Seleccionado
23-2014	07-2014-08-025	No Seleccionado	Seleccionado
23-2014	24-2012-07-009	No Seleccionado	Seleccionado
23-2014	15-2011-07-016	No Seleccionado	Seleccionado
23-2014	23-2014-07-192	No Seleccionado	Seleccionado
23-2014	24-2012-07-042	No Seleccionado	Seleccionado
23-2014	12-2012-07-008	No Seleccionado	Seleccionado
23-2014	23-2014-07-033	No Seleccionado	Seleccionado
23-2014	15-2013-07-026	No Seleccionado	Seleccionado
23-2014	15-2011-07-062	No Seleccionado	Seleccionado
23-2014	23-2014-07-156	No Seleccionado	Seleccionado
23-2014	02-2014-07-030	No Seleccionado	Seleccionado
23-2014	02-2014-07-032	No Seleccionado	Seleccionado
23-2014	23-2014-07-152	No Seleccionado	Seleccionado
23-2014	15-2013-07-054	No Seleccionado	Seleccionado
23-2014	15-2013-07-016	No Seleccionado	Seleccionado
23-2014	02-2014-07-034	No Seleccionado	Seleccionado
23-2014	02-2014-07-003	No Seleccionado	Seleccionado
23-2014	15-2013-07-037	No Seleccionado	Seleccionado
23-2014	15-2013-07-007	No Seleccionado	Seleccionado
23-2014	21-2013-08-067	No Seleccionado	Seleccionado
23-2014	07-2013-08-066	No Seleccionado	Seleccionado

Fuente: Elaborado por la Contraloría General de acuerdo a los antecedentes proporcionados por la Comisión Nacional de Riego, en relación con el registro de modificaciones realizadas a la información de la base de datos en productivo del Sistema Electrónico Ley 18.450.

ANEXO N° 6

Muestra de modificaciones efectuadas a las variables de proyectos que participaron en la simulación de puntajes oficial de concurso.

Código Concurso	Fecha de Apertura	Hora de Apertura	Fecha de Modificación	Hora de Modificación	Código Proyecto	Aporte	Superficie Ponderada	Costo	Período en que se efectuó la modificación
19-2014	17-10-2014	10:00	16-10-2014	11:24:35	19-2014-02-002	15	1,76	2,362	Antes de la Fecha de Apertura
19-2014	17-10-2014	10:00	17-10-2014	11:47:09	19-2014-02-002	15	1,76	2,36	Después de la Fecha de Apertura
19-2014	17-10-2014	10:00	20-10-2014	17:18:28	19-2014-02-002	15	1,76	2356,01	Después de la Fecha de Apertura
19-2014	17-10-2014	10:00	3-11-2014	12:30:58	19-2014-02-002	15	1,76	2362,14	Modificación Final después de la Fecha de Apertura
19-2014	17-10-2014	10:00	16-10-2014	11:30:08	19-2014-02-004	25	2,48	4,718	Antes de la Fecha de Apertura
19-2014	17-10-2014	10:00	17-10-2014	11:47:09	19-2014-02-004	25	2,48	4,72	Después de la Fecha de Apertura
19-2014	17-10-2014	10:00	20-10-2014	17:18:28	19-2014-02-004	25	2,48	4706,03	Después de la Fecha de Apertura
19-2014	17-10-2014	10:00	4-11-2014	16:05:08	19-2014-02-004	25	2,48	4718,27	Modificación Final después de la Fecha de Apertura
19-2014	17-10-2014	10:00	16-10-2014	16:29:41	19-2014-11-001	13	6	6,135	Antes de la Fecha de Apertura
19-2014	17-10-2014	10:00	17-10-2014	10:03:12	19-2014-11-001	13	6	6,14	Después de la Fecha de Apertura
19-2014	17-10-2014	10:00	24-10-2014	14:20:53	19-2014-11-001	13	6	6119,35	Después de la Fecha de Apertura
19-2014	17-10-2014	10:00	29-10-2014	12:54:38	19-2014-11-001	13	6	6135,27	Modificación Final después de la Fecha de Apertura
20-2014	5-11-2014	10:00	4-11-2014	17:55:33	20-2014-07-013	12,51	3,86	1,761	Antes de la Fecha de Apertura
20-2014	5-11-2014	10:00	5-11-2014	10:22:28	20-2014-07-013	12,51	3,86	1,76	Después de la Fecha de Apertura
20-2014	5-11-2014	10:00	6-11-2014	10:44:11	20-2014-07-013	12,51	3,86	1761,77	Modificación Final después de la Fecha de Apertura
20-2014	5-11-2014	10:00	4-11-2014	18:21:02	20-2014-06-008	20	4,04	3,146	Antes de la Fecha de Apertura
20-2014	5-11-2014	10:00	5-11-2014	10:22:28	20-2014-06-008	20	4,04	3,15	Después de la Fecha de Apertura
20-2014	5-11-2014	10:00	5-11-2014	10:43:59	20-2014-06-008	20	4,04	3146,83	Modificación Final después de la Fecha de Apertura
20-2014	5-11-2014	10:00	4-11-2014	18:38:15	20-2014-04-011	23,1	4,46	6,017	Antes de la Fecha de Apertura
20-2014	5-11-2014	10:00	5-11-2014	10:22:28	20-2014-04-011	23,1	4,46	6,02	Después de la Fecha de Apertura

Código Concurso	Fecha de Apertura	Hora de Apertura	Fecha de Modificación	Hora de Modificación	Código Proyecto	Aporte	Superficie Ponderada	Costo	Período en que se efectuó la modificación
20-2014	5-11-2014	10:00	5-11-2014	12:27:59	20-2014-04-011	23,1	4,46	6017,74	Modificación Final después de la Fecha de Apertura
22-2014	19-11-2014	10:00	14-11-2014	18:56:00	09-2014-07-008	29,95	45,38	4518,24	Antes de la Fecha de Apertura
22-2014	19-11-2014	10:00	16-12-2014	19:27:14	09-2014-07-008	33,5	45,38	4518,24	Modificación Final después de la Fecha de Apertura
22-2014	19-11-2014	10:00	18-11-2014	23:44:37	22-2014-04-051	40	16,67	2,014	Antes de la Fecha de Apertura
22-2014	19-11-2014	10:00	19-11-2014	9:41:34	22-2014-04-051	40	16,67	2,01	Antes de la Fecha de Apertura
22-2014	19-11-2014	10:00	20-11-2014	16:34:44	22-2014-04-051	40	16,67	2014,36	Modificación Final después de la Fecha de Apertura
22-2014	19-11-2014	10:00	18-11-2014	21:28:29	22-2014-07-025	31,01	13,69	3,238	Antes de la Fecha de Apertura
22-2014	19-11-2014	10:00	19-11-2014	9:41:33	22-2014-07-025	31,01	13,69	3,24	Antes de la Fecha de Apertura
22-2014	19-11-2014	10:00	20-11-2014	16:36:58	22-2014-07-025	31,01	13,69	3238,9	Modificación Final después de la Fecha de Apertura
23-2014	12-12-2014	10:00	3-12-2014	1:38:50	23-2014-07-032	46,88	55,63	8,02	Antes de la Fecha de Apertura
23-2014	12-12-2014	10:00	21-01-2015	12:48:12	23-2014-07-032	46,88	55,63	8020,67	Modificación Final después de la Fecha de Apertura
23-2014	12-12-2014	10:00	11-12-2014	20:42:24	23-2014-07-189	20,21	41,51	4,884	Antes de la Fecha de Apertura
23-2014	12-12-2014	10:00	12-12-2014	13:17:56	23-2014-07-189	20,21	41,51	4,88	Después de la Fecha de Apertura
23-2014	12-12-2014	10:00	26-01-2015	15:54:38	23-2014-07-189	20,21	41,51	4884,95	Modificación Final después de la Fecha de Apertura
23-2014	12-12-2014	10:00	1-12-2014	12:24:37	23-2014-07-004	46,88	10,44	1,659	Antes de la Fecha de Apertura
23-2014	12-12-2014	10:00	12-12-2014	13:17:55	23-2014-07-004	46,88	10,44	1,66	Después de la Fecha de Apertura
23-2014	12-12-2014	10:00	8-01-2015	15:09:18	23-2014-07-004	46,88	10,44	1659,99	Modificación Final después de la Fecha de Apertura

Fuente: Elaborado por Contraloría General de acuerdo a los antecedentes suministrados por la Comisión Nacional de Riego, mediante el registro de modificaciones realizadas a la información de la base de datos productiva del Sistema Electrónico Ley 18.450.

ANEXO N° 7

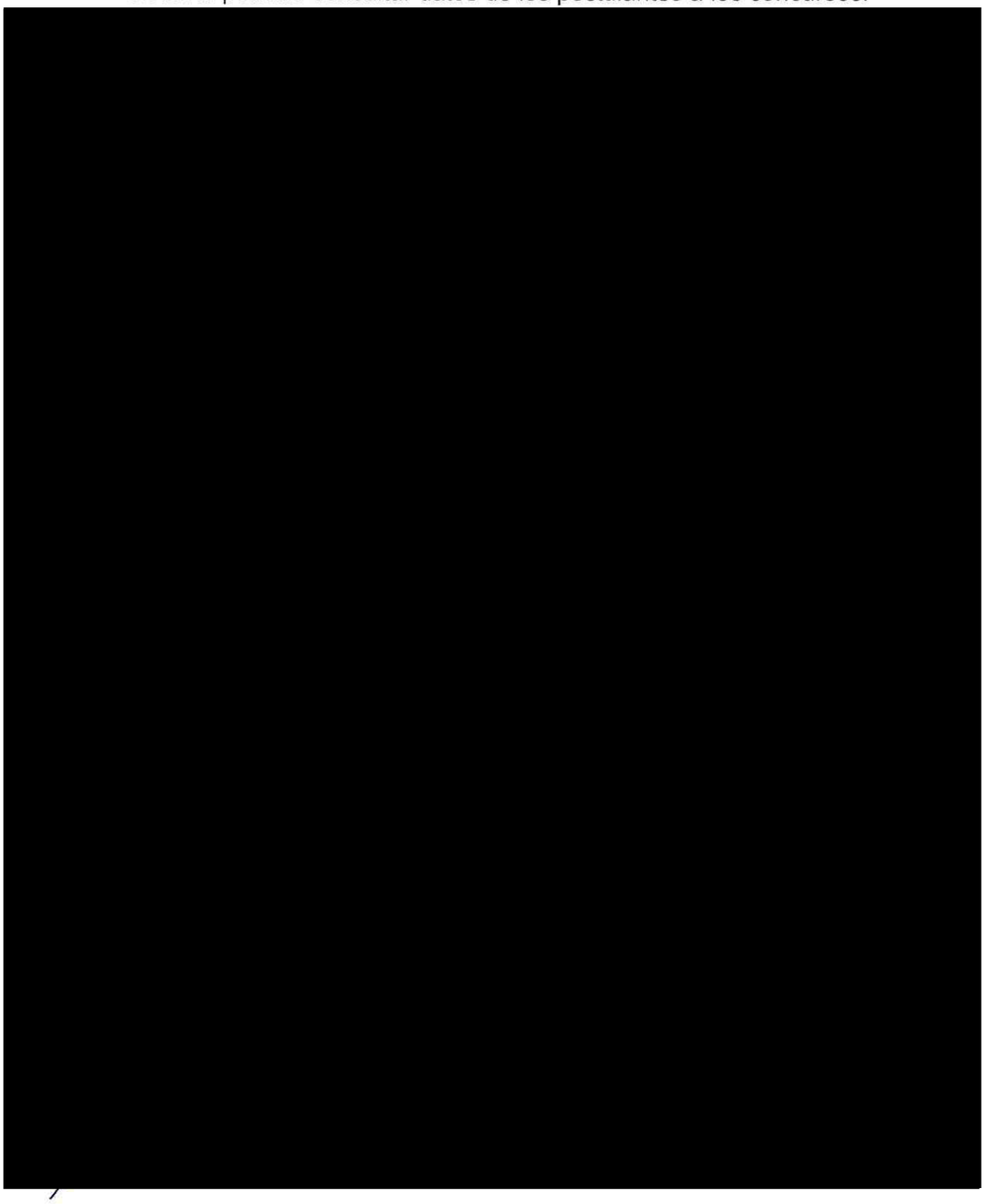
Muestra de hallazgos del Informe Final de Auditoría N° 00120141, de 28 de febrero de 2014, efectuado por la empresa Decalink Ltda., los cuales al 25 de abril no han sido subsanados.

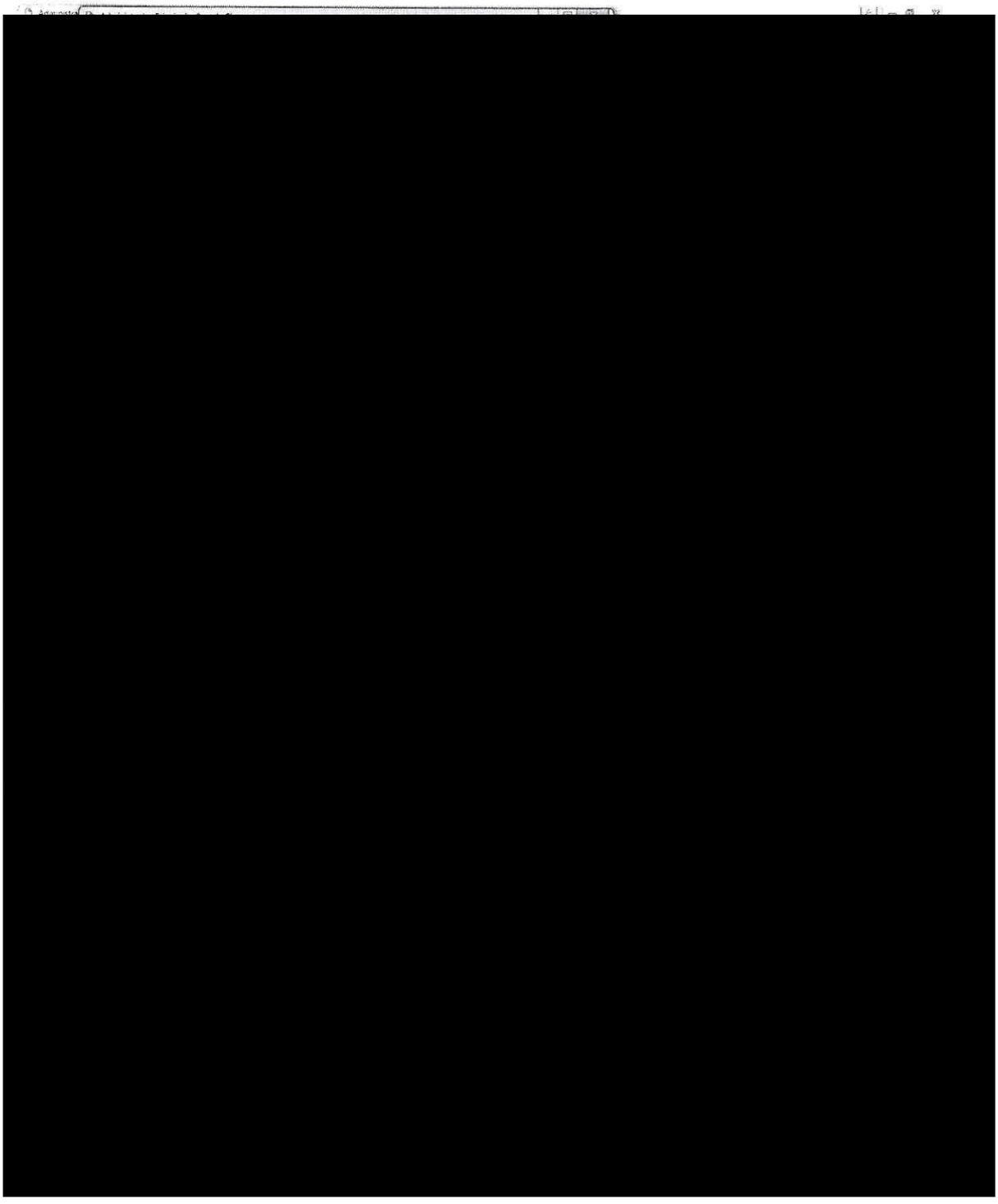
Menú Afectado	Nombre de Perfil	Sección Informe	Subsección Informe
Reportes y Consultas / Búsquedas / Búsquedas de Personas y Entidades	Superadministrador	4.2	4.2.1
Reportes y Consultas / Gestión / Monto Resolución Concursos	Superadministrador	4.2	4.2.1
Postulación / Proyectos / Ingreso y Mantención	Consultor	4.4	4.4.1
Evaluación / Consultor / Retirar Proyecto	Consultor	4.5	4.5.1
Adjudicación / Publicación / Publicar Listados	Superadministrador	4.7	4.7.1
Adjudicación / Reclamaciones / Ingreso Solicitud Consultor / Ficha Solicitudes Enviadas	Superadministrador	4.7	4.7.1
Seguimiento / Inicio de Obra / Mis avisos de inicio de obras	Superadministrador	4.9	4.9.1
MT / Mantención Usuario / Revisión Solicitudes	Superadministrador	4.11	4.11.1

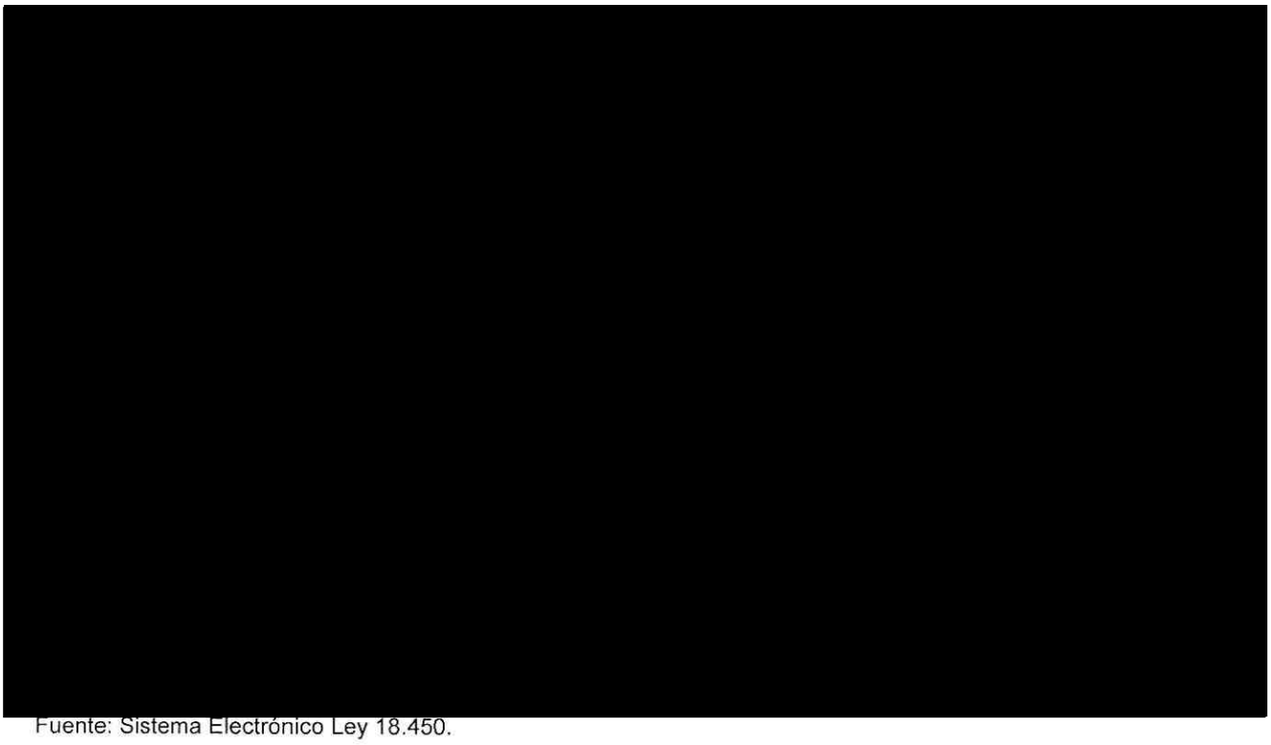
Fuente: Elaborado por Contraloría General de acuerdo a los antecedentes respaldados en el Informe Final N° if00120141, de 28 de febrero de 2014, sobre auditoría al Sistema Electrónico Ley 18.450.

ANEXO N° 8

Sistema permite consultar datos de los postulantes a los concursos.







Fuente: Sistema Electrónico Ley 18.450.

ANEXO N° 9

Detalle de los contratos TI convenidos por la CNR, vigentes durante el período de la auditoría.

SERVICIO CONTRATADO	PROYECTO SISTEMA LEY; JBOSS FUSE SERVICE WORK 16 CORE STANDARD Y JBOSS BPM SUITE 16 CORE STANDARD	RED HAT JBOSS ENTERPRISE APPLICATION PLATFORM 16 CORE STANDARD	ENLACE MPLS 20 MB INTERCONEXIÓN SANTIAGO, LA SERENA, TEMUCO Y CHILLÁN	SERVICIO MANTENCIÓN PLATAFORMA UNIBOX AÑO 2015
Nombre del proveedor	COMPUTACION E INGENIERIA S.A.	COMPUTACION E INGENIERIA S.A.	CLARO SERVICIOS EMPRESARIALES S.A.	SOCIEDAD DE TECNOLOGÍAS DE LA INFORMACIÓN EXCEED LTDA.
RUT del proveedor	96.693.120-5	96.693.120-5	95.714.000-9	77.766.870-6
Identificador mercado público	2239-4-LP10	2239-4-LP10	870-13-LE14	2239-4-LP10
Resolución que aprueba las bases	Resolución N° 24, de 28 de marzo de 2011.	Resolución N° 24, de 28 de marzo de 2011.	Resolución N° 69, de 31 de diciembre de 2012.	Resolución N° 24, de 28 de marzo de 2011.
Resolución que adjudica	No aplica	No aplica	No aplica	No aplica
Resolución que aprueba el contrato	No aplica	No aplica	No aplica	No aplica
Identificador del contrato	870-965-CM14	870-981-CM14	870-441-SE14	870-118-CM15
Monto total de la adquisición	US$ 68.544	US$ 6.640,2	$ 4.548.180	US$ 28.241,2
Modalidad de pago	Otro.	Otro.	30 días contra la recepción conforme de la factura.	Otro.
Duración del contrato	36 meses	12 meses	12 meses	36 meses
Tipo de caución	Boleta Bancaria pagadera a la vista.	Boleta Bancaria pagadera a la vista.	Boleta Bancaria, depósito a la vista, vale vista o certificado de fianza a la vista.	Boleta Bancaria pagadera a vista.
Beneficiario	Dirección de Compras y Contratación Pública.	Dirección de Compras y Contratación Pública	Dirección de Compras y Contratación Pública.	Dirección de Compras y Contratación Pública
Monto caución	$ 1.000.000	$ 1.000.000	UF 200	$ 1.000.000
Tipo de multas	Por atrasos en la entrega los Ítems o productos, las cuales podrán hacerse efectiva a través de descuentos en el respectivo pago.	Por atrasos en la entrega los Ítems o productos, las cuales podrán hacerse efectiva a través de descuentos en el respectivo pago.	Por atrasos en la entrega de los servicios de Hosting (Máquinas Virtuales), Housing y servicios adicionales, o por la indisponibilidad de estos.	Por atrasos en la entrega los Ítems o productos, las cuales podrán hacerse efectiva a través de descuentos en el respectivo pago.
Definición de multa	Cláusula octava de las bases de licitación pública, sobre multas.	Cláusula octava de las bases de licitación pública, sobre multas.	Punto 10.13, sobre Multas y sanciones.	Cláusula octava de las bases de licitación pública, sobre multas.

Fuente: Elaborado por la Contraloría General con los antecedentes proporcionados por la CNR, a través el Oficio N° 2.648, de 20 de agosto de 2015, e información del sitio web de Mercado Público.

CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
UNIDAD DE AUDITORÍA DE SISTEMAS

ANEXO N° 10

Estado de Observaciones del Informe Final N° 305, de 2016.

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
II. Examen de la Materia Auditada numeral 1.	Falta de mecanismos de revisión periódica a la integridad de la información.	C: Observación Compleja, Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres de 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	A la CNR le corresponderá desarrollar y sancionar mecanismos de revisión periódica a la integridad de la información del Sistema Electrónico Ley 18.450, suministrando un informe de avance a esta Entidad de Control en el término de 60 días hábiles contados desde la recepción del presente informe final.			
II. Examen de la Materia Auditada numeral 2.	Omisión de pruebas al plan de continuidad del negocio.	C: Observación Compleja, Inexistencia de planes de contingencia.	El servició deberá informar del resultado de al menos una prueba realizada al plan de continuidad del negocio, en un plazo máximo de 60 días hábiles, contados a partir de la recepción del presente informe, en donde se identifique claramente que los riesgos expuestos en el plan fueron analizados y el resultado final de estas pruebas.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
II. Examen de la Materia Auditada numeral 3.	Carencia de un programa de actualización al plan de contingencia.	AC: Observación Altamente Compleja, Inexistencia de planes de contingencia.	La entidad deberá actualizar el aludido plan y agregar un control de cambios al documento, en donde se identifique la fecha y responsable de cada una de sus versiones. Adicionalmente, una vez culminado el proceso de actualización, este documento tendrá que ser formalizado y suministrado a esta entidad fiscalizadora, en un plazo máximo de 60 días hábiles, contados desde la recepción del presente informe.			
II. Examen de la Materia Auditada numeral 4.	Falta de controles físicos considerados en el procedimiento de control de acceso a la sala de servidores.	C: Observación Compleja, Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres de 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	La Comisión Nacional de Riego deberá actualizar y formalizar el procedimiento de control de acceso al datacenter, a fin de considerar los hechos expuestos en la observación, junto con establecer las medidas correctivas atingentes al hallazgo, debiendo informar de sus avances a este organismo de control, en un plazo de 60 días hábiles, contados desde la recepción del presente informe final.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
II. Examen de la Materia Auditada numeral 5.	Debilidades en el control de acceso a redes externas.	C: Observación Compleja, Falta de políticas de resguardo de la información o que estas no se encuentren formalizadas.	El servicio deberá suministrar en un plazo de 60 días, documentación que evidencie las medidas adoptadas para que a nivel de firewall, se restrinja la conexión a sitios y protocolos que permitan la descarga de contenido no confiable en internet, tales como mega.nz y BitTorrent. Esto debe ser aplicado tanto para equipos externos como internos conectados a internet mediante el uso de la red institucional.			
II. Examen de la Materia Auditada numeral 6.	Ausencia de estrategias de recuperación ante desastres.	AC: Observación Altamente Compleja, Inexistencia de planes de contingencia.	La CNR deberá incorporar los distintos planes de recuperación atingente a cada uno de los sistemas críticos del plan de contingencia, suministrando dicho documento formalizado en un plazo de 60 días hábiles, contados desde la recepción del presente informe.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
II. Examen de la Materia Auditada numeral 7.	Carencia de una política que instruya sobre el uso del correo electrónico institucional.	C: Observación Compleja, Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres de 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	La CNR tendrá que desarrollar y sancionar una política que instruya sobre el uso del correo electrónico institucional, acreditando la medida en el plazo de 60 días hábiles, contados desde la recepción del presente informe.			
II. Examen de la Materia Auditada numeral 8.	Falta de un proceso formal de inducción a las medidas de seguridad TI adoptadas por la institución.	C: Observación Compleja, Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	La repartición deberá elaborar y formalizar de manera documental el citado proceso de capacitación, suministrándolo a este Organismo de Control en el plazo de 60 días hábiles, contados desde la recepción de este informe final.			
II. Examen de la Materia Auditada numeral 9.	Falta de seguridad en el sitio externo de almacenamiento	C: Observación Compleja, Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres del 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	La institución deberá efectuar las evaluaciones técnicas correspondientes a la viabilidad de la implementación de las acciones correctivas, informado sus estados de avance en el plazo de 60 días hábiles, contados desde la recepción de este informe final.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
II. Examen de la Materia Auditada numeral 12.	Autentificación débil en el Sistema Electrónico Ley 18.450.	AC: Observación Altamente Compleja, Falencias de seguridad de sistemas.	La Comisión Nacional de Riego deberá actualizar todas las contraseñas administradas en el sistema, comunicando las medidas adoptadas y acompañando los antecedentes de respaldo respectivos, en un plazo máximo de 60 días hábiles, contados desde la recepción de este informe.			
II. Examen de la Materia Auditada numeral 13.	Falta de revisión de los permisos de acceso.	AC: Observación Altamente Compleja, Falencias de seguridad de sistemas.	La entidad deberá llevar cabo un proceso de revisión de usuarios desvinculados en cada uno de los sistemas críticos institucionales, como también, actualizar y posteriormente formalizar el procedimiento denominado Gestión de Acceso a Redes Locales y Servicio Mensajería Electrónica, debiendo informar del estado de avance, en el mismo plazo de 60 días hábiles, contados desde la recepción de este informe.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
II. Examen de la Materia Auditada numeral 15.	Deficiencia en el control y gestión del inventario TI	C: Observación Compleja, Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres de 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	La CNR tendrá que realizar una revisión del inventario de los servidores físicos, en conjunto con el área responsable de activos del servicio, constatando el correcto registro de cada activo, identificando como mínimo, número de inventario, número de serie, modelo, ubicación física y características técnicas, confirmando la medida en el plazo de 60 días hábiles, contados desde la recepción de este informe final.			
II. Examen de la Materia Auditada numeral 16.	Falencias en el control de acceso al Sistema Electrónico Ley 18.450.	AC: Observación Altamente Compleja, Falencias de seguridad de sistemas.	Considerando que actualmente existen concursos en ejecución, la repartición deberá analizar y solucionar las vulnerabilidades asociadas a la manipulación de parámetros en los enlaces del aplicativo web, informando el estado de avance de esta evaluación y posterior implementación, en un plazo máximo de 60 días hábiles, contados desde la recepción de este reporte.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
II. Examen de la Materia Auditada numeral 17.	Ausencia de controles que restrinjan el cambio de perfilamiento.	AC: Observación Altamente Compleja, Falencias de seguridad de sistemas.	La Comisión Nacional de Riego deberá evaluar y corregir lo advertido, informando el estado de avance en lo relativo al análisis e implementación de medidas correctivas en el sistema, en un plazo máximo de 60 días hábiles, contados desde la fecha de recepción del presente informe.			
II. Examen de la Materia Auditada numeral 18.	Falla de controles de acceso a información confidencial de proyectos.	AC: Observación Altamente Compleja, Falencias de seguridad de sistemas.	La CNR deberá tomar medidas tendientes a solucionar las brechas de seguridad detectadas, a fin de resguardar la confidencialidad de la información, evaluando el estado actual del sistema, informando de los avances dentro del plazo de 60 días hábiles, contados desde la recepción del presente informe.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
II. Examen de la Materia Auditada numeral 19.	Deficiencia de controles de acceso a la base de datos.	AC: Observación Altamente Compleja, Falencias de seguridad de sistemas.	La CNR deberá establecer un procedimiento para llevar un registro de los cambios realizados y aprobados por la jefatura del Departamento de Fomento al Riego, informando del avance en un plazo máximo de 60 días hábiles, contados desde la recepción del presente reporte.			
II. Examen de la Materia Auditada numeral 20.	Hallazgo de vulnerabilidad sin subsanación.	AC: Observación Altamente Compleja, Falencias de seguridad de sistemas.	La Comisión Nacional de Riego deberá realizar la reparación del software en estudio, respecto a las debilidades indicadas en los correos electrónicos del 10 y 23 de diciembre de 2013, informándose a este Ente de Control en un periodo de 60 días hábiles, contados desde la recepción del presente informe.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
II. Examen de la Materia Auditada numeral 21.	Cierre de incidencia sin medida adoptada.	AC: Observación Altamente Compleja, Falencias de seguridad de sistemas.	El servicio deberá analizar la corrección de la incidencia descrita en el ticket N° 318 de 2012, informando su estado de avance, en el plazo de 60 días hábiles, contados desde la recepción del presente informe final.			
II. Examen de la Materia Auditada numeral 23.	Vulnerabilidades de seguridades informadas en la auditoría externa en el año 2014 y no subsanadas.	AC: Observación Altamente Compleja, Falencias de seguridad de sistemas.	Le corresponderá a la repartición definir y sancionar un procedimiento de atención de incidencias que registre las acciones tomadas por el encargado de seguridad. Asimismo, deberá regularizar todas las fallas de seguridad expuestas en el Anexo N° 9, remitiendo a esta Contraloría General, en ambos casos, el informe de avance en un plazo máximo de 60 días, contados desde la fecha de recepción del presente informe.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
II. Examen de la Materia Auditada numeral 24.	Sistema permite consultar datos de los postulantes a concursos a través del formulario de búsqueda.	AC: Observación Altamente Compleja, Falencias de seguridad de sistemas.	La institución auditada deberá levantar un análisis de las causales de la falla de seguridad, junto con informar el estado de avance de las medidas correctivas aplicadas, en un período de 60 días hábiles, contados desde la recepción del presente informe.			
II. Examen de la Materia Auditada numeral 25.	Falta de eficacia al contratar productos Red Hat para la creación de la nueva versión del Sistema Electrónico Ley 18.450	C: Observación Compleja, Existencia de actos, que causan detrimento fiscal.	El servicio deberá informar el estado de avance del nuevo aplicativo, al que se refiere en su respuesta, en el término de 60 días hábiles.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
II. Examen de la Materia Auditada numeral 27.	Deficiencias en la seguridad física del site principal de la CNR.	C: Observación Compleja: Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres de 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	• Desarrollar y sancionar un procedimiento formal de control de acceso, para registrar al personal que ingresa a las instalaciones, solicitando su cédula de identidad o pasaporte. • Separar los cables de comunicación y de corriente eléctrica, a fin de mitigar la interferencia del tráfico de datos. • Disponer un perímetro para la sala de servidores, de concreto o material sólido. • Incorporar en dicho lugar, alarmas en puertas y sensores de movimiento, de forma tal de evitar eventuales robos, pérdidas de información y equipos de procesamiento. • Instalar dispositivos que permitan detectar la existencia de humo, humedad, y alzas de temperatura. • Disponer un sistema contra incendios del tipo eléctrico.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
II. Examen de la Materia Auditada numeral 27.	Deficiencias en la seguridad física del site principal de la CNR.	C: Observación Compleja: Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres de 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	• Certificar la mitigación del riesgo de fugas de agua dentro de la ubicación del equipamiento de la institución, por una entidad del rubro. • Señalizar instrucciones relativas al consumo de alimentos, bebidas, tabaco y medios de grabación, en las cercanías de los dispositivos informáticos. Para todas ellas deberá informar su estado de avance, en un plazo de 60 días hábiles, contados desde la recepción del presente informe final.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
II. Examen de la Materia Auditada numeral 28.	Deficiencias en la seguridad física del site de contingencia del servicio.	C: Observación Compleja, Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres de 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	• Disponer un perímetro para la sala de servidores, de concreto o material sólido. • Separar los cables de comunicación y de corriente eléctrica, a fin de mitigar la interferencia del tráfico de datos. • Incorporar en dicho lugar, alarmas en puertas y sensores de movimiento, de forma tal de evitar eventuales robos, pérdidas de información y equipos de procesamiento. • Colocar un sensor detector de humo. • Certificar la mitigación del riesgo de fugas de agua dentro de la ubicación del equipamiento de la institución, por una entidad del rubro. • Señalizar instrucciones relativas al consumo de alimentos, bebidas, tabaco y medios de grabación, en las cercanías de los dispositivos informáticos.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
II. Examen de la Materia Auditada numeral 28.	Deficiencias en la seguridad física del site de contingencia del servicio.	C: Observación Compleja, Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres de 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	• Instalar en el site mencionado, una puerta contra fuego. El estado de avance de tales medidas deberá ser informado a esta Entidad de Control en el plazo de 60 días hábiles, contados desde la recepción del presente informe.			
II. Examen de la Materia Auditada numeral 29.	Falta de registro de actividades efectuadas en el Sistema Electrónico Ley 18.450.	C: Observación Compleja: Incumplimiento de la normativa contenida en los decretos N^{os} 77, 81 y 83, los tres de 2004; 93 y 100, ambos de 2006, todos del Ministerio Secretaría General de la Presidencia.	La CNR tendrá que incorporar al software en cuestión, la funcionalidad de registrar los nombres de los usuarios que realicen transacciones sensibles dentro del aplicativo, detallando fecha y hora, acción realizada y terminal utilizado, acreditando la medida en el plazo de 60 días hábiles, contados desde la recepción del presente informe.			

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
II. Examen de la Materia Auditada numeral 21.	Cierre de incidencia sin medida adoptada.	AC: Observación Altamente Compleja, Falencias de seguridad de sistemas.	La CNR deberá instruir un sumario administrativo a fin de establecer posibles responsabilidades en relación al cierre del ticket N° 318, situación que fue alertada durante el año 2012, sin que el personal responsable tomara las medidas de resguardo tendientes a evitar cualquier vulnerabilidad en el sistema; a las vulnerabilidades de seguridades informadas en la auditoría externa en el año 2014 y no subsanadas, lo que ha infringido la normativa que sustenta las bases de los concursos N^{os} 19-2014, 20-2014, 22-2014 y 23-2014; a la adquisición de los servicios asociados a la orden de compra ID N° 870-981-CM14, de 30 de diciembre de 2014; a la			
II. Examen de la Materia Auditada numeral 22.	Modificaciones en las variables de postulación posterior a la fecha de apertura.	AC: Observación Altamente Compleja, Falencias de seguridad de sistemas.				
II. Examen de la Materia Auditada numeral 25.	Falta de eficacia al contratar productos Red Hat para la creación de la nueva versión del Sistema Electrónico Ley 18.450	C: Observación Compleja, Existencia de actos, que causan detrimento fiscal.				

N° OBSERVACIÓN SEGÚN INFORME FINAL	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN O VERIFICAR MEDIDAS ADOPTADAS	MEDIDA ADOPTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DEL SERVICIO
II. Examen de la Materia Auditada numeral 30.	Omisión en la definición de una fecha de vencimiento para hacer exigible el eventual cobro por concepto de garantía por la prestación de las órdenes de compra ID N^{os} 870-117-CM15 y 870-118-CM15.	C: Observación Compleja, Incumplimiento de normativa relacionada con el proceso de compra.	omisión en la definición de una fecha de vencimiento para hacer exigible el eventual cobro por concepto de garantía por la prestación de las órdenes de compra ID N^{os} 870-117-CM15 y 870-118-CM15, y a la inexistencia de documentación para ejecutar el examen de las eventuales multas asociadas a las órdenes de compra ID N^{os} 870-965-CM14 y 870-981-CM14, remitiendo a este Organismo de Control, en el término de 15 días hábiles contado desde la recepción del presente informe, el acto administrativo mediante el cual se disponga tal proceso y se designe al fiscal.			
II. Examen de la Materia Auditada numeral 31.	Inexistencia de documentación para ejecutar el examen de las eventuales multas asociadas a las órdenes de compra ID N^{os} 870-965-CM14 y 870-981-CM14.	C: Observación Compleja, Incumplimiento de normativa relacionada con el proceso de compra.				

www.contraloria.cl