



CONTRALORÍA GENERAL DE LA REPÚBLICA
 DIVISIÓN DE INFRAESTRUCTURA Y REGULACIÓN
 SUBDIVISIÓN DE AUDITORÍA

DIR : 1.150/10
 REF.: 236.872/10

REMITE INFORME FINAL DE
 OBSERVACIONES N° 50, DE 2010,
 SOBRE AUDITORÍA DE SISTEMAS
 REALIZADA EN LA COMISIÓN
 NACIONAL DE RIEGO.

M. Jara
- Antecedente a los efectos
20-10-10

SANTIAGO, 15.OCT 10 *061652

Cumpro con enviar a Ud., para su conocimiento y fines legales pertinentes, el informe final N° 50, del año en curso, de la auditoría de sistemas realizada en la Comisión Nacional de Riego.

Sobre el particular, corresponde que esa Comisión adopte las medidas respectivas con el objeto de superar las observaciones planteadas en los términos previstos en el citado informe final, cuya efectividad será verificada por esta Contraloría General en futuras fiscalizaciones.

Saluda atentamente a Ud.,

Patricio Vera

COMISION NACIONAL DE RIEGO OFICINA DE PARTES	
N° 7796	Código 104702
Fecha	19 OCT 2010

POR ORDEN DEL CONTRALOR
 GENERAL DE LA REPUBLICA
 DIVISION DE INFRAESTRUCTURA Y REGULACION
 SUBJEFE DIVISION
 SUBROGANTE

AL SEÑOR
 SECRETARIO EJECUTIVO DE LA
 COMISIÓN NACIONAL DE RIEGO
 PRESENTE.

RTE
 ANTECED

CONTRALORÍA GENERAL DE LA REPÚBLICA
División de Infraestructura y Regulación

Informe Final
Comisión Nacional de Riego



Fecha: 13 OCT. 2010
N° Informe: 50/2010



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE INFRAESTRUCTURA Y REGULACIÓN
SUBDIVISIÓN DE AUDITORÍA

DIR : 1.150/10
REF. : 236.872/10
PMET : 15.047/10

INFORME FINAL N° 50, SOBRE AUDITORÍA
DE SISTEMAS REALIZADA EN LA COMISIÓN
NACIONAL DE RIEGO.

SANTIAGO, 13 OCT 2010

En cumplimiento del plan anual de fiscalización para el presente año, esta Contraloría General efectuó una auditoría de sistemas en la Comisión Nacional de Riego, durante el período comprendido entre el 2 al 13 de agosto del presente año, en virtud de lo dispuesto en el artículo 16, de la ley N°10.336.

Objetivo.

La auditoría tuvo por finalidad realizar un catastro de los sistemas de información que apoyan los procesos del servicio y evaluar los controles de seguridad de la información en el ámbito de la confidencialidad y disponibilidad.

Metodología.

El examen se practicó conforme a las normas de control interno y de auditoría aprobadas por esta Contraloría General mediante resoluciones exentas N°s 1.485 y 1.486, ambas de 1996, y se desarrolló de acuerdo con los procedimientos establecidos en la metodología de auditoría de este Organismo Fiscalizador.

La seguridad de la información se evaluó en conformidad con lo consignado en el decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia y su norma relacionada NCh-ISO 27002.Of2009 -declarada oficial de la República de Chile por resolución exenta N° 1.535, de 27 de agosto de 2009, del Ministerio de Economía, Fomento y Reconstrucción-, que reemplaza a la norma NCh2777.Of 2003, ambas del Instituto Nacional de Normalización.

Universo.

Está constituido por diez sistemas de información, a saber:

A LA SEÑORA
PATRICIA MEZA VILLEGAS
SUBJEFE DE LA DIVISIÓN DE INFRAESTRUCTURA Y REGULACIÓN (S)
PRESENTE.
MEM/SIM/ERV

Contraloría General
de la República



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE INFRAESTRUCTURA Y REGULACIÓN
SUBDIVISIÓN DE AUDITORÍA

1. Sistema de administración beneficios Ley N° 18.450 de Fomento al Riego y Drenaje
2. Sistema de registro de seguimiento de documentos
3. Sistema de recursos humanos
4. Sistema de administración de incidentes y soporte computacional
5. Sistema de administración de documentos para la gestión de calidad
6. Sistema de búsqueda documental bibliográfica para la ciudadanía
7. Sistema de planificación y control de gestión
8. Sistema de gestión de solicitudes de consulta ciudadana
9. Sistema de información geográfico
10. Sistema de activo fijo

Muestra.

Se realizaron pruebas a los controles de la seguridad de información de las primeras cuatro aplicaciones computacionales definidas en el universo, que representan un 40% del total.

Antecedentes Generales.

El decreto ley N° 1.172, de 1975, cuyo texto refundido fue fijado por el decreto con fuerza de ley N° 7, de 1983, del Ministerio de Economía, creó la Comisión Nacional de Riego como persona jurídica de derecho público, relacionada con el ejecutivo a través del Ministerio de Agricultura. A partir de 1985, se incorporó a sus funciones la administración de la ley N° 18.450, que fomenta las obras privadas de construcción y reparación de obras de riego y drenaje y promueve el desarrollo agrícola de los productores de las áreas beneficiadas.

La Comisión Nacional de Riego tiene por misión "contribuir al desarrollo de la agricultura a través del riego y drenaje, mediante la formulación e implementación de la política, estudios, programas y proyectos que aporten con un carácter inclusivo y de equidad, al mejoramiento de la competitividad de los agricultores, agricultoras y organizaciones regantes".

Dicho servicio está organizado en un consejo de ministros integrado por los titulares de Agricultura – quien lo preside –, Economía, Fomento y Reconstrucción, Hacienda, Obras Públicas, y Planificación. Además,



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE INFRAESTRUCTURA Y REGULACIÓN
SUBDIVISIÓN DE AUDITORÍA

cuenta con una Secretaría Ejecutiva, la cual tiene como función principal ejecutar los acuerdos que el consejo adopte.

Acorde a su actual estructura organizacional, establecida mediante la resolución exenta N° 2.098, del año en curso, de la Comisión Nacional de Riego, la Secretaría Ejecutiva está conformada por las divisiones de Estudios, Desarrollo y Políticas, y Jurídica, y por los departamentos de Fomento al Riego, y Administración y Finanzas.

Los servicios tecnológicos son entregados por la Unidad de Gestión Informática, dependiente jerárquicamente del Departamento de Administración y Finanzas, que cumple labores de desarrollo y mantenimiento de los sistemas centrales, soporte de usuarios y resolución de incidentes, mantención de la infraestructura de redes y comunicaciones, administración de contratos con empresas externas, entre otras.

La infraestructura de red de datos y comunicaciones de la Comisión Nacional de Riego se representa en el siguiente esquema.

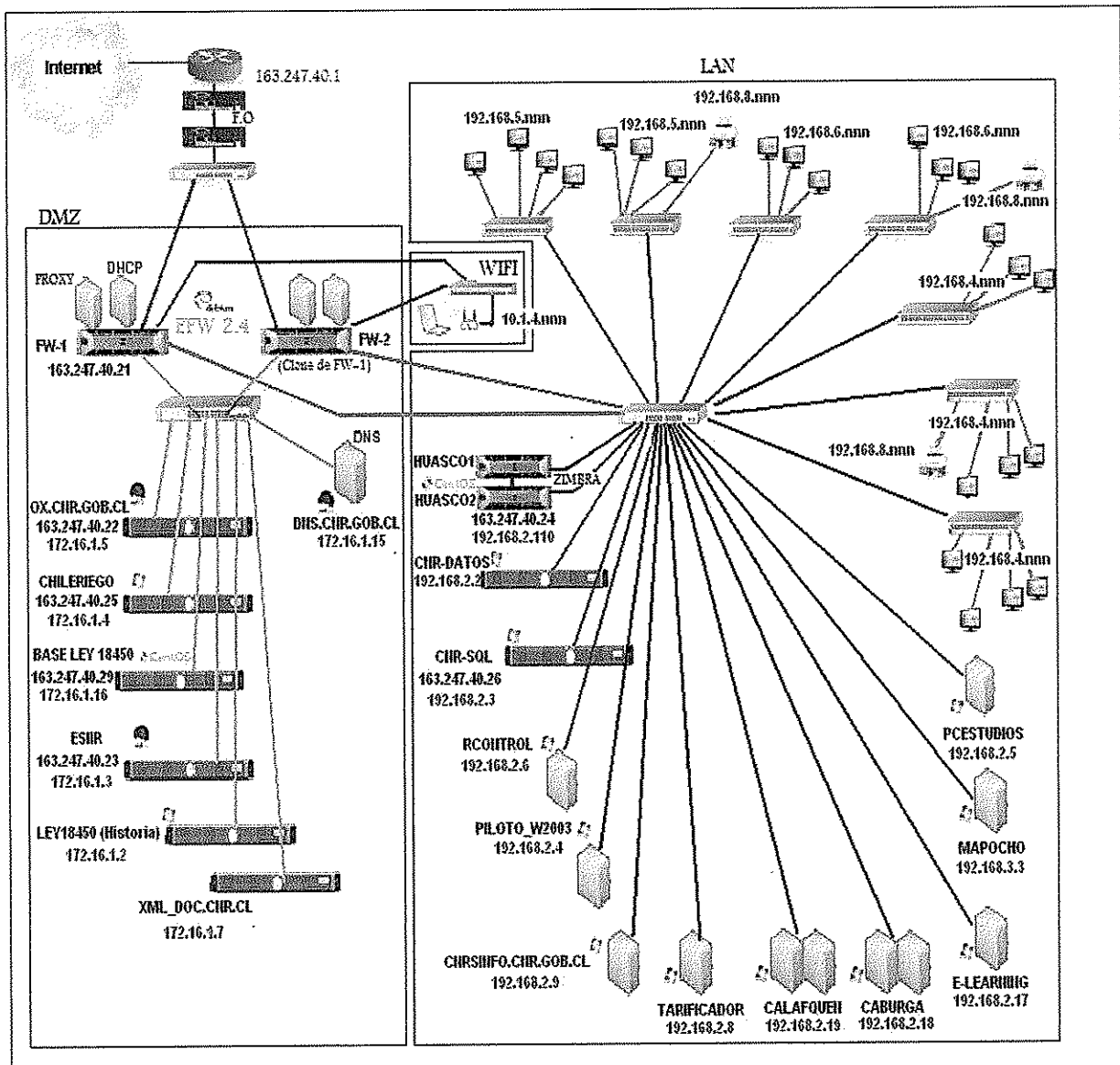


Figura N° 1: Diagrama de red y comunicaciones (Fuente: Unidad de Gestión Informática)



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE INFRAESTRUCTURA Y REGULACIÓN
SUBDIVISIÓN DE AUDITORÍA

En el anexo de este informe se especifican para cada uno de los sistemas mencionados en el acápite "Universo", los procesos que éstos apoyan y sus características más relevantes.

El resultado del examen realizado dio origen al preinforme de observaciones que fue puesto en conocimiento del Secretario Ejecutivo de la Comisión Nacional de Riego, mediante oficio N° 50.923, del año en curso, de este Organismo Contralor.

Posteriormente, dicha autoridad dio respuesta a través de oficio N° 4.070, del presente año, cuyos argumentos y antecedentes han sido considerados en la preparación del presente informe final.

De la revisión efectuada a los sistemas e instalaciones computacionales de la Comisión Nacional de Riego se determinaron las siguientes observaciones:

EVALUACIÓN DE CONTROLES GENERALES TI.

1.1 CONTROLES DE ACCESO LÓGICO.

1.1.1 Deficiencias detectadas en relación a la formulación de contraseñas.

En las pruebas realizadas a los sistemas de información, se verificó que los usuarios pueden crear contraseñas sin restricciones de tamaño o complejidad. En efecto, se comprobó que los sistemas auditados admiten tanto el ingreso de contraseñas desde largo uno como secuencia de caracteres iguales, lo que no se ajusta a lo establecido en la norma NCh-ISO 27002.Of2009, numeral 11.3.1, letra d, según el cual el usuario debe seleccionar contraseñas de calidad con una extensión determinada, libres de caracteres idénticos sucesivos, sean éstos numéricos o alfanuméricos, que ofrezcan suficiente garantía de inviolabilidad.

El servicio auditado, expone en su respuesta, que esta deficiencia será abordada como prioridad inmediata para aplicar en los principales sistemas de la institución, en la medida que disponga de los recursos presupuestarios necesarios.

Este Organismo de Control, por el momento, mantiene lo observado mientras no se compruebe la efectividad de las medidas que se adopten, en una próxima auditoría de seguimiento.

1.1.2 Falta de control respecto a la actualización periódica de contraseñas.

Se constató que no se encuentran activos en los sistemas de información auditados, los mecanismos de control que exijan al usuario el cambio de su contraseña cada cierto periodo de tiempo y que impidan la reutilización de éstas, lo que vulnera lo establecido en la precitada norma, numeral 11.3.1 letra e, el cual indica que se deben cambiar las contraseñas a intervalos regulares, manteniendo un registro de las antiguas, para evitar su reutilización.

Al respecto, la Comisión Nacional de Riego, junto con reconocer la deficiencia, informa que cuenta con una propuesta de



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE INFRAESTRUCTURA Y REGULACIÓN
SUBDIVISIÓN DE AUDITORÍA

Reglamento de Seguridad Informática, elaborado entre otros, por el Comité de Seguridad Informática, actualmente en proceso de validación por las áreas asesoras del servicio, que establece como regla "que las claves de acceso de los usuario(a) a la red interna deberá ser cambiada cada 90 días. Lo anterior deberá ser recordado al usuario(a) de manera automática y pudiendo el usuario(a) realizar este cambio de clave antes del plazo estipulado".

Considerando lo argumentado por la entidad, se mantiene, por el momento, lo objetado, hasta que no se verifique la real implementación de las medidas anunciadas, conforme los programas de seguimiento de esta Entidad de Control.

1.1.3 Deficiencias en la generación de contraseñas temporales.

En la revisión efectuada a los sistemas de información se comprobó que el procedimiento de creación de contraseñas temporales no incorpora mecanismos de generación con claves aleatorias, no cumpliendo con lo estipulado en la norma antes mencionada, numeral 11.2.3, letra e, que indica que las contraseñas temporales deben ser únicas para cada usuario y no descifrables.

En su respuesta, la entidad fiscalizada acepta lo observado y agrega que será planteado en reuniones de coordinación, con el objeto de alcanzar un procedimiento formal para la habilitación de password temporales.

En consecuencia, se mantiene lo objetado, mientras no se evalúen las medidas que se adopten, en una próxima auditoría de seguimiento.

1.1.4 Debilidades en el cambio de contraseña inicial.

Se verificó que el sistema no avisa automáticamente a los usuarios que se conectan por primera vez a los sistemas de información, respecto a cambiar las contraseñas primitivas, transgrediendo lo indicado en la norma ya citada, numeral 11.2.3, letra b, que dispone que los usuarios con cuentas de acceso nuevas, deben contar inicialmente de una contraseña temporal, la que luego de ingresarla, debería cambiarse, según advertencia del propio sistema.

El servicio señala que esta situación será abordada a partir de la implementación de su Reglamento de Seguridad Informático. Por ende, no es posible en esta instancia, subsanar la objeción, y será materia de análisis de una futura auditoría de seguimiento.

1.2 CONTINUIDAD DE LAS OPERACIONES.

1.2.1 Falta aseguramiento de la continuidad operacional.

El sistema de administración de beneficios de la ley N° 18.450, está alojado en un servidor que no cuenta con características de alta disponibilidad, lo que impide su actualización, con riesgo de pérdida de la información



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE INFRAESTRUCTURA Y REGULACIÓN
SUBDIVISIÓN DE AUDITORÍA

y discontinuidad operacional, con el consiguiente impacto para la institución y los usuarios externos que utilizan dicho sistema.

El servicio fiscalizado informa que incluyó en la formulación presupuestaria para el año 2011, la implementación de una plataforma de virtualización que permita alcanzar las características de alta disponibilidad exigida.

Ponderado lo expuesto por el servicio, se fiscalizará la efectiva implementación de la plataforma mencionada en una próxima auditoría, manteniéndose, por el momento, lo observado.

1.2.2 Inexistencia de un plan de contingencia y recuperación.

La administración no ha diseñado un plan que contrarreste eventuales interrupciones para así proteger sus procesos críticos ante fallas importantes de los sistemas de información, asegurando su pronta restauración, situación que no se ciñe a lo establecido en la norma NCh-ISO 27002.Of2009, numeral 14.1.3 letras (a, b, c, d, e, f y g).

Al respecto, la institución auditada reconoce la deficiencia observada y manifiesta, que se ha incluido en la cartera preliminar de proyectos del Programa de Mejoramiento de la Gestión de Seguridad de la Información a ejecutar a contar del año 2011, la implementación de una Virtualización y Storage, que permitirá asegurar la disponibilidad de la infraestructura TICs y generar las condiciones necesarias para realizar regularmente las pruebas de recuperación de sus componentes.

En virtud de los antecedentes aportados, no es posible entender superada la objeción, mientras no se constate en una próxima fiscalización, la efectiva solución anunciada sobre la materia.

Conclusión.

La Comisión Nacional de Riego, ha aceptado íntegramente las observaciones contenidas en este informe. Adicionalmente, estableció someter a discusión presupuestaria para el ejercicio 2011, las inversiones requeridas para superarlas.

Considerando lo anterior esta Contraloría General, evaluará los resultados de las acciones que el servicio implemente en una futura auditoría de seguimiento.

Saluda atentamente a Ud.,

DIVISION DE INFRAESTRUCTURA Y REGULACION
JEFE SUBDIVISION DE AUDITORIA
SUBROGANTE



ANEXO

CATASTRO DE SISTEMAS DE INFORMACIÓN DE LA COMISIÓN NACIONAL DE RIEGO

Nombre del sistema	Departamento	Proceso asociado	Responsable de mantención	Tipo de contrato	Duración del contrato	Tipo de alojamiento	Ubicación del alojamiento
Sistema de administración beneficios de Ley N° 18.450 de Fomento al Riego y Drenaje	Fomento al Riego	Subsidios	Interplus SA.	Soporte a todo evento 5x9	Diciembre 2010	Interno	Sala de Servidores
Sistema de registro de seguimiento de documentos	Administración y Finanzas	Flujo de trabajo de documentos	CEGE SA.	Soporte externo contra evento	N/A	Interno	Sala de Servidores
Sistema de recursos humanos	Administración y Finanzas	Gestión de personal, remuneraciones y control de asistencia	CEGE SA.	Soporte externo contra evento	N/A	Interno	Sala de Servidores
Sistema de administración de incidentes y soporte computacional	Informática	Soporte de servicios tecnológicos	Informática	Soporte interno permanente	N/A	Interno	Sala de Servidores

CONTRALORÍA GENERAL DE LA REPÚBLICA
 DIVISIÓN DE INFRAESTRUCTURA Y REGULACIÓN
 SUBDIVISIÓN DE AUDITORÍA



Nombre del sistema	Departamento	Proceso asociado	Responsable de mantención	Responsable de mantención	Duración del contrato	Tipo de alojamiento	Ubicación de alojamiento
Sistema de administración de documentos para la gestión de calidad	Secretaría Ejecutiva	Repositorio de documentos	Grupo Norte	Soporte a todo evento 7x24	Diciembre 2010	Interno	Sala de Servidores
Sistema de búsqueda documental bibliográfica para la ciudadanía	Administración y Finanzas	Repositorio de documentos	WYNISIS	Soporte interno permanente	N/A	Interno	Sala de Servidores
Sistema de planificación y control de gestión	Planificación	Administración	BALEY	Soporte externo contra evento	N/A	Interno	Sala de Servidores
Sistema de gestión de solicitudes de consulta ciudadana	Comunicaciones	Información a la ciudadanía	SEGPRES	Soporte permanente 5x9	N/A	Interno	Sala de Servidores
Sistema de información geográfico	Estudios	Estudio de proyectos	SIIG SA.	Soporte a todo evento 5x9	Diciembre 2010	Interno	Sala de Servidores
Sistema de activo fijo	Administración y Finanzas	Registro y control de inventario	Patricio Ulloa Justiniano	Soporte externo contra evento	N/A	Interno	Sala de Servidores

[Handwritten signature]

OFICIO N° 4070 /

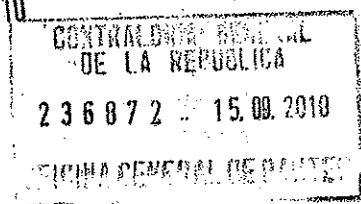
ANT.: Oficio N° 50923, de 01 de Septiembre de 2010, de Contraloría General de La República, que remite preinforme de observaciones N° 50, de 2010, sobre auditoría de sistemas realizada en la Comisión Nacional de Riego.

Mat.: Informa.

Santiago, 13 SEP 2010

DE : SECRETARIO EJECUTIVO
COMISIÓN NACIONAL DE RIEGO

A : MARÍA ISABEL CARRIL CABALLERO
SUB JEFE DIVISIÓN DE INFRAESTRUCTURA Y REGULACIÓN
CONTRALORÍA GENERAL DE LA REPÚBLICA



Con fecha 01 de Septiembre de 2010, se ha recibido por esta jefatura Oficio individualizado en antecedentes por el cual se remite preinforme de observaciones N° 50, de 2010, sobre auditoría de sistemas realizada en la Comisión Nacional de Riego.

Sobre el particular y respondiendo a dicho Oficio, debo señalar lo siguiente:

1. EVALUACIÓN DE CONTROLES GENERALES TI:

En su informe se señala que una vez realizadas pruebas de los sistemas de información se verificó que:

- 1.1 Los usuarios pueden crear contraseñas sin restricciones de tamaño o complejidad, lo que supone una contravención a la norma NCh-ISO 27002.OF 2009, numeral 11.3.1 letra D: Al respecto debo informar que actualmente nos encontramos en primera etapa del PMG de Seguridad de la Información el cual ya nos ha requerido como institución un reporte que de cuenta de un diagnóstico institucional. Este PMG en la materia y, respecto del Dominio de Control de Acceso, recomienda elegir identificadores que tengan una longitud mínima de ocho caracteres; sean fáciles de recordar; contengan letras, mayúsculas, dígitos, y caracteres de puntuación; no estén basados en cosas obvias o de fácil deducción a partir de datos relacionados con la persona, por ejemplo, nombres, números telefónicos, cédula de identidad, fecha de nacimiento; estén libres de caracteres idénticos consecutivos o grupos completamente numéricos o alfabéticos; y no sean palabras de diccionario o nombres comunes.
- En nuestro diagnóstico institucional reconocemos la existencia de una brecha, declarada, consistente en la inexistencia de un mecanismo automatizado que permita ejercer controles en esta materia, además de la falta de una orientación formal al respecto. Esta brecha será abordada como prioridad inmediata para aplicar en los principales sistemas de nuestra institución en la medida de que se dispongan de los recursos presupuestarios pertinentes.
- Sin perjuicio de lo anterior, en la actualidad y con las herramientas que actualmente se encuentran disponibles, cada vez que se crea una nueva cuenta de usuario, el usuario recibe una serie de recomendaciones que permitan paliar las deficiencias informadas. Junto con ello y en el corto plazo se realizarán reuniones de coordinación con los respectivos clientes de los sistemas de información a fin de abordar las alternativas de solución y lograr un plan de ejecución que permitan dar solución a este hallazgo. Una vez verificado este plan de ejecución será debidamente informado.

1.2 Falta de control respecto a la actualización periódica de contraseñas: Este Servicio cuenta con una propuesta de Reglamento de Seguridad Informática el que ha sido elaborado en conjunto por el Comité de Seguridad Informática, propuesta que sobre el particular indica que "...se establece como regla que las claves de acceso de usuario(a) a la red interna deberán ser cambiadas cada 90 días. Lo anterior deberá ser recordado al usuario(a) de manera automática y pudiendo el usuario(a) realizar este cambio de clave de acceso antes del plazo estipulado".

Esta Política de Seguridad esta siendo validada por las áreas asesoras del Servicio para su posterior sanción y difusión entre el personal.

De igual forma reconocemos que existe una brecha al no existir los mecanismos de control automatizado que exija al usuario el cambio de periódico de su contraseña y que impidan la reutilización de éstas.

En el corto plazo se realizarán reuniones de coordinación con los respectivos clientes de los sistemas de información a fin de abordar las alternativas de solución y lograr un plan de ejecución que considerará a lo menos, lo siguiente:

- o Para los usuarios internos de la CNR deberán habilitarse las directivas de contraseñas con objetos de Directiva de Grupo.
- o Para los usuarios externos de CNR (conectados directamente desde la red pública) deberán implementarse en cada uno de los sistemas de información un mecanismo de control de Vigencia máxima de las contraseñas.

En ambos casos se deberá exigir a los proveedores de los Sistemas de Información la implementación de este control.

1.3 Deficiencias en la generación de contraseñas temporales:

Efectivamente en gran parte de nuestros sistemas de información aún no incorporan los mecanismos de generación de claves aleatorias, situación que también será abordada en las reuniones de coordinación con los respectivos clientes de los sistemas de información.

En tal sentido el objetivo es alcanzar el procedimiento formal para la habilitación de claves provisorias las que tendrán asociadas propuestas de generación de credenciales randomicas

1.4 Debilidades en el cambio de contraseña inicial: Efectivamente en gran parte de nuestros sistemas de información aún no se incorporan los mecanismos de notificación automática informando a los usuarios que se conecten por primera vez a los sistemas de información deban cambiar las contraseñas primitivas, situación que será abordada a partir de la implementación de nuestro Reglamento de Seguridad Informático.

Avda. Libertador Bernardo O'Higgins N° 1449 - 4º Piso

Teléfono: 425 79 00 - Fax: 425 79 01 - 425 79 03 - 425 79 05 - Casilla 424 - V, Correo 21, Santiago - Chile

www.cnr.cl

Junto con ello y en breve plazo se realizarán reuniones de coordinación con los respectivos encargados/responsables de los sistemas de información a fin de abordar las alternativas de solución que desde los parámetros que impondrá el Reglamento de Seguridad a que se hace referencia, deberá contemplar a lo menos los siguientes aspectos:

- Para los usuarios internos de la CNR serán habilitados los mecanismos de notificación cambio de contraseña inicial que será ejecutado cada vez que un usuario sea incorporado al dominio (para el caso de la incorporación de un nuevo usuario a la institución)
- Para los usuarios externos de CNR (conectados directamente desde la red pública) su clave de acceso inicial a sistemas de información será notificada vía correo electrónico para que luego sea obligatorio del cambio de contraseña por parte del usuario.

En ambos casos se deberá exigir a los proveedores de los Sistemas de Información la implementación de este control.

2. CONTINUIDAD DE LAS OPERACIONES

2.1 Falta de aseguramiento de la continuidad operacional:

Efectivamente el sistema de administración de beneficios de la ley N° 18.450, esta alojado en un servidor que aún no cuenta con características de alta disponibilidad.

Esta situación ya ha sido relevada anteriormente dentro de nuestra organización y en efecto fue señalada en la formulación presupuestaria 2011 a fin de poder implementar una plataforma de virtualización que permita alcanzar las características de alta disponibilidad exigidas.

A la fecha esta situación no ha podido ser abordada en atención a las restricciones presupuestarias del Servicio.

En virtud de lo anterior, con el principal cliente de este sistema de información se ha coordinado una reunión para la tercera semana de Septiembre con el fin de abordar este y otros temas de seguridad de acceso a fin de implementar una alternativa de solución en el corto plazo, resultados que serán informados en su oportunidad.

Avda. Libertador Bernardo O'Higgins N° 1449 - 4º-Piso

Teléfono: 425 79 00 - Fax: 425 79 01 - 425 79 03 - 425 79 05 - Casilla 424 - V, Correo 21, Santiago - Chile

www.cnr.cl

2.2 Inexistencia de un plan de contingencia y recuperación:

Efectivamente en nuestra institución aún no se ha logrado abordar completamente la Gestión de la Disponibilidad de la infraestructura.

A la fecha sólo se ha podido declarar la Política de Respaldo y Recuperación de la Información y en paralelo se ha logrado reemplazar y mejorar el Sistema de Respaldo Automático de la infraestructura. Por otra parte, y tal como fue indicado, el nuevo PMG de Seguridad de la Información, respecto del Dominio de Gestión de Operaciones y Comunicaciones señala que: "Deberá garantizarse la disponibilidad de infraestructura adecuada de respaldo, para asegurar que éstos estén disponibles incluso después de un desastre o la falla de un dispositivo. Las configuraciones de respaldo para los sistemas individuales deberán ser probadas con regularidad, a lo menos cada 2 años, para asegurar que ellas satisfacen los requisitos estipulados en los planes de continuidad institucionales"

En este aspecto, existe una brecha declarada dado que se encuentran pendientes de realizar los procedimientos y ambientaciones necesarias para ejecutar las pruebas y validaciones de recuperación, lo ya fue declarado en la cartera preliminar de proyectos del referido PMG lo que en la especie importa la necesidad de implementar una Virtualización y Storage que permitirá asegurar la disponibilidad de la Infraestructura TICs y generar las condiciones necesarias para realizar regularmente las pruebas de recuperación de los componentes de la infraestructura TICs.

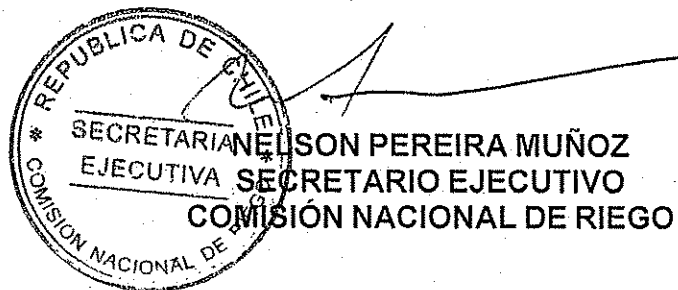
Efectivamente la CNR presenta brechas en materia de gestión de TICs y las mismas han sido relevadas tanto a vuestro órgano de control como en el marco del PMG de Seguridad de la Información.

En este contexto se está trabajando a fin de, con las disponibilidades presupuestarias con que se cuenta y las herramientas que nos entrega la Ley, generar los mecanismos de control o herramientas paliativas que sean del caso.

Resulta relevante que los hallazgos informados sean vistos a la luz de los requerimientos que plantea el PMG de Seguridad de la Información pues la etapa en que actualmente se encuentra (diagnostico institucional) nos permitirá generar una cartera de proyectos cuya ejecución y planificación inicial está pensada para el 2011 y con metas de ejecución al 2012.

Muchos de estos proyectos y soluciones pasan por la necesaria destinación de recursos presupuestarios de ahí que nuestro diagnóstico sincero y certero nos permite definir líneas de acción institucional que a mediano plazo nos lleve a solucionar las brechas detectadas.

Es todo cuanto puedo informar a Ud.



[Handwritten signature]
PLUE/MJG/MSG/CCA/FAR.

DISTRIBUCION

- Contraloría General de la República
- Administración y Finanzas
- Oficina de Partes

102571



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE INFRAESTRUCTURA Y REGULACIÓN
SUBDIVISIÓN DE AUDITORÍA

DIR : 1.150/10
REF.: 236.872/10

REMITE INFORME FINAL DE
OBSERVACIONES N° 50, DE 2010,
SOBRE AUDITORÍA DE SISTEMAS
REALIZADA EN LA COMISIÓN
NACIONAL DE RIEGO.

SANTIAGO,

Cumplo con enviar a Ud., para su conocimiento y fines legales pertinentes, el informe final N° 50, del año en curso, de la auditoría de sistemas realizada en la Comisión Nacional de Riego.

Sobre el particular, corresponde que esa Comisión adopte las medidas respectivas con el objeto de superar las observaciones planteadas en los términos previstos en el citado informe final, cuya efectividad será verificada por esta Contraloría General en futuras fiscalizaciones.

Saluda atentamente a Ud.,

POR ORDEN DEL CONTRALOR
GENERAL DE LA REPUBLICA
DIVISION DE INFRAESTRUCTURA Y REGULACION
SUBJEFE DIVISION
SUBROGANTE

att
AL SEÑOR
SECRETARIO EJECUTIVO DE LA
COMISIÓN NACIONAL DE RIEGO
PRESENTE.