Energía

Gobierno de Chile

SUPERINTENDENCIA DE ELECTRICIDAD Y COMBUSTIBLES

10251

ORD: N° _____ / ACC 904390 / DOC 665536 /

CONTRALORIA GENERAL
OFICINA GENERAL DE PARTES
14 NOV 2013

ANT.: Informe Final N° 2 del 8 de agosto de 2013 de la Contraloría General de la República.

MAT.: Remite respuesta sobre auditoria de sistemas de la Superintendencia de Electricidad y Combustibles.

SANTIAGO, 13 NOV. 2013

DE : SUPERINTENDENTE DE ELECTRICIDAD Y COMBUSTIBLES (SEC)

A : ABOGADA JEFA DE LA DIVISIÓN DE AUDITORÍA ADMINISTRATIVA DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA
SRA. MARIA ISABEL CARRIL CABALLERO

En respuesta al informe Final No.2 de la Contraloría General de la República de fecha 8/08/2013 que tuvo por finalidad revisar y evaluar aspectos que se relacionan con las políticas, normas, prácticas y procedimientos de control vinculados a las Tecnologías de la Información y Comunicaciones, nos permitimos señalar a Ud. lo siguiente, en el mismo orden de las observaciones planteadas:

I. Decreto No. 83, de 2004, del MINSEGPRES.

a) En lo referente a lo indicado en la letra a), de dicho Informe, SEC indica que "se realizará una modificación al documento denominado Política de Seguridad Institucional, contenido en la resolución exenta No. 2.120 del 26-10-2012, especificando los mecanismos de difusión del mismo", podemos informar lo siguiente:

- Se realizó la modificación a la Política de Seguridad de acuerdo a lo solicitado (Res. Ex. N° 1526 del 02/07/2013, ver anexo N° 1), en esta se especifica "La Superintendencia (SEC) realiza actividades periódicas de difusión y entrenamiento de políticas de Seguridad de la información a los distintos estamentos de su personal", "Las políticas se publican en intranet de la SEC", "además se realiza una charla semestral, a través de la cual se capacita al personal de la institución, en las materias relativas a la Política de Seguridad".

  Durante el año 2013 se realizó difusión de ésta y otras políticas y procedimientos relacionados con la Seguridad de Información, a través de correo electrónico enviado por la Unidad de Comunicaciones el 19/08/2013 (ver Anexo 2) y se publicó en Intranet de SEC con la misma fecha, adicionalmente se dispusieron los links para descargar los documentos (ver Anexo No. 3).

Adicionalmente, es preciso señalar la realización de jornadas de capacitación los días 29 de julio, 21 y el 23 de octubre de 2013 con la participación de funcionarios de la institución (ver Anexo 4).

La próxima, de acuerdo a planificación, está programada para el 20 de diciembre de 2013, con ello se concluiría durante el 2013 estas jornadas de capacitación.

En cuanto a lo mencionado en el párrafo 3 de la misma letra a), que señala "se confeccionará una orden de servicio, con instrucciones sobre el consumo de alimentos, bebidas y otros elementos que puedan afectar los sistemas informáticos" podemos indicar lo siguiente:

La "política específica de Seguridad de pantalla y escritorios limpios" se formalizó a través de la Res. Ex. N° 0808 del 03/04/2013. En esta se especifica, entre otros temas que "se prohíbe el consumo de alimentos y bebidas junto a los sistemas informáticos tales como servidores, notebooks, tablets, computadores de escritorio, unidades de almacenamiento u otro similar" (ver anexo 5).

Esta materia, como todas las que involucra la Política de Seguridad de la Información, han sido abordadas en las jornadas de capacitación realizadas, que da cuenta el párrafo anterior de esta presentación y las que se encuentran evidenciadas en el Anexo 3.

b) Respecto a lo mencionado en la letra b), de Informe Final No.2, podemos indicar que se realizó la modificación de la Política de Seguridad (Res. Ex. N° 1526 del 02/07/2013, (ver en anexo 1), de acuerdo a lo solicitado, donde se especifican las recomendaciones para la generación y cuidado de las contraseñas, entre otras se indica:
   - " - mantener la confidencialidad de las contraseñas de aplicaciones y sistemas cuando así se le indique, las que para todos los efectos son personales e intransferibles. La asignación de contraseñas se deberá controlar a través de un proceso formal de gestión a cargo del Área de soporte, las recomendaciones son:
     - ✓ No escribir en papeles de fácil acceso, ni en archivos sin cifrar.
     - ✓ No habilitar la opción "recordar clave en este equipo", que ofrecen los programas.
     - ✓ No enviarla por correo electrónico.
     - ✓ Nunca guardar las contraseñas en ningún tipo de papel, agenda, etc.
     - ✓ Las contraseñas se deben mantener confidenciales en todo momento.
     - ✓ No compartir las contraseñas con otros usuarios
   - Cambiar las contraseñas si se sospecha que alguien más la conoce y que ha tratado de hacer mal uso de ella.
   - Seleccionar contraseñas que no sean fáciles de adivinar.
   - Cambiar las contraseñas regularmente.
   - No utilizar contraseñas con números telefónicos, nombre de familia, etc.

- Reportar violaciones de la seguridad de información al Encargado de Seguridad de la Información."

c) En lo concerniente a la letra c), se puede indicar que SEC formalizó una "Política Específica de control de acceso de información (R.E 809 del 03/04/2013, ver anexo N° 6)" donde se especifican las reglas y deberes de los usuarios en cuanto al control para el acceso a la información, acceso a instalaciones de procesamiento de información, documentos electrónicos, redes y sistemas informáticos, la cual fue publicada en la intranet y se envió por medio del correo institucional.

Ésta como el resto de las materias que forman parten de la Política de Seguridad de la información contenidas en el D.S. N° 83, han sido abordadas en las jornadas de capacitación efectuadas con los funcionarios y que da cuenta, como lo hemos dicho, el Anexo 3 de esta presentación.

d) En lo relativo a la letra d) sobre las comunicaciones entre la Superintendencia y las autoridades de emergencia, puedo informar que se encuentran contenidas en cada uno de los Planes de emergencia denominados "PLAN DE EMERGENCIA Y EVACUACIÓN SEC", correspondiente en cada una de las sedes del Servicio, es decir, Direcciones Regionales, Oficinas Provinciales y oficinas del nivel central (tres). Estos documentos se encuentran publicados en la intranet institucional, http://intranet2.sec.cl/prevencion-de-riesgos/. A manera ejemplar se adjunta Plan de Emergencia de la Oficina Central (ver Anexo N° 7).

Sin perjuicio de lo anterior, y con el objetivo de dar cabal cumplimiento a las materias contenidas en el Art. 35 del Decreto 83, la Unidad de Informática de la institución está elaborando un catastro de documentos electrónicos y sistemas informáticos con definición de responsables lo que será contenido en los Planes de Contingencia y matriz de riesgo simplificada de la institución actualizada al primer semestre de 2014.

e) En lo referido en la letra e) se puede informar que se realizó una modificación a la Política de Seguridad (Res. Ex. N° 1526 20/07/2013), en ella se especifica que "La Política será revisada y evaluada anualmente, lo que se verificará en el mes de noviembre de cada año, desde su aprobación por el Comité de Seguridad de la Información, quien propondrá las modificaciones pertinentes al Superintendente, si corresponde". (ver Anexo 1)

En virtud a lo señalado en el párrafo anterior, la revisión y evaluación de la Política de Seguridad, debe ejecutarse por el Comité de Seguridad de la información durante este mes, noviembre, y si correspondiere, proponer los ajustes y actualizaciones a dicha política institucional.

f) En lo concerniente a la acreditación de las referencias del personal que posee acceso a los equipos de procesamiento de datos y a las que manipulan información sensible, letra f, señalar que se ha procedido a incluir el siguiente texto (formalizado a través del Memorando ACC 888489 de la aplicación TIMES, ver Anexo 11), el que está siendo efectivo a partir de los procesos de fecha 1° de octubre de 2013:

"El o los Adjudicatarios, sus consultores y personal directo que se encuentren ligados a los proyectos que resulten de este Convenio, en alguna de sus etapas, deberán guardar absoluta confidencialidad sobre los antecedentes, reservados o no, que de la Entidad contratante conozcan durante su desarrollo. La responsabilidad del adjudicado será solidaria respecto de sus personeros, empleados, consultores o subcontratistas.

El proveedor adjudicado deberá tomar las medidas que considere necesarias para el resguardo de la confidencialidad de la información, reservándose la Entidad contratante el derecho a ejercer acciones legales que correspondan de acuerdo a las normas legales vigentes.

La divulgación, por cualquier medio, de la totalidad o parte de la información referida por parte de la(s) empresa(s) adjudicada(s) durante la vigencia del contrato o después de su finalización, dará lugar a la Entidad contratante a entablar acciones judiciales que correspondan contra el proveedor, sin perjuicio de la responsabilidad solidaria por los actos en infracción de esta obligación que hayan ejecutados sus empleados."

En cuanto a la mantención de autorizaciones a sistemas informáticos, señalar que la Unidad de Informática se encuentra desarrollando los procedimientos para solicitar la baja, modificaciones o altas de acceso a los sistemas de información. Esto será difundido de acuerdo a las políticas de difusión de la Institución. Adicionalmente se establecerá en el procedimiento el Registro del otorgamiento de claves de acceso.

Sin perjuicio de lo señalado en el párrafo anterior e independiente que el procedimiento, integralmente, estará implementado a partir de abril de 2014, señalar que el registro de otorgamiento de claves se encontrará disponible a contar del 1° de diciembre de 2013.

g) En cuanto a lo señalado en el Informe Final N° 2, que los equipos computacionales que se usan fuera de la organización no se encuentran asegurados por compañías del rubro, es preciso indicar que mediante Memorando 892118, de fecha 21/05/2012 (ver Anexo N° 14) el Sub Departamento de Administración de esta Superintendencia, informa que no ha sido factible encontrar una compañía que entregue una póliza con estas características, puesto que en general los productos ofrecidos dicen relación con todos los activos institucionales, en estas circunstancias se reitera el

criterio utilizado en el memorando 826338 de fecha 21 de marzo de 2013, en orden a no contratar una póliza de seguro (ver Anexo N° 12).

h) En cuanto a lo señalado en la letra i) del Informe Final N° 2, indicar la implementación de una mejora en el proceso relacionado con el personal que ingresa a la Institución, consistente en:

En los contratos de personal se ha procedido de la siguiente manera (formalizada mediante Memorando ACC 884644 de la plataforma TIMES, (ver Anexo N° 8):

- Contratos a honorarios: A partir del mes de abril del año 2013 se incorporó la cláusula séptima en los convenios a honorarios, donde se establece confidencialidad en el uso de información, la obligación de accesar sólo a los sistemas a los que se encuentra autorizado y la sanción en caso de incumplimiento (ver Anexo N° 9).

- Nombramientos de Planta y Contrata: A partir de los nombramientos del mes de octubre del 2013 se ha agregado una Declaración Jurada a los documentos que deben completar los funcionarios al incorpore a la Institución (ver Anexo N° 10).

i) En cuanto al análisis del Plan de contingencia, el departamento de informática ha realizado un cronograma de actividades que consta de las siguientes etapas:

1. Noviembre 2013: Revisión y actualización del actual Plan de Contingencia.
2. Diciembre 2013: Identificación del impacto de los eventos en los procesos críticos de acuerdo a la Matriz de Riesgo institucional, y evaluación de dependencia de los eventos que puedan afectar estos procesos y su costo.
3. Abril 2014: Simulación controlada en la ejecución de los Planes de contingencia y ajustes si corresponde.

II. Incumplimiento de decretos, Decreto No. 93, de 2006 del MINSEGPRES.

En relación a lo observado en el numeral 2 del Informe Final No. 2, puede indicarse que se realizará una modificación al procedimiento de rebaja de usuarios de los sistemas de información de SEC, donde se incluirá las actividades que se deben realizar para la reconfiguración de las cuentas de correos de los funcionarios desvinculados. La implementación en el servidor de correo electrónico institucional será realizada por personal de SEC. Este procedimiento será publicado en la intranet y difundido por correo electrónico. Plazo: Diciembre 2013.

III. Incumplimiento Decreto No. 100, de 2006 del MINSEGPRES.

En cuanto a lo observado en el numeral 3 del Informe Final No. 2, puede indicarse que se ha definido un plan de acción que considera 2 etapas:

a) Identificación y clasificación de errores sobre la estructura de las hojas de estilo en cascada, y del sitio Web. Octubre a diciembre 2013.

b) Corrección de errores Enero - Abril 2014.

c) Adicionalmente se ha instruido a la Unidad de Comunicaciones de SEC que todas las páginas nuevas que se agreguen al sitio, se deben construir bajo el estándar especificado en la letra a) (ver Anexo N° 13).

Hacemos presente, que la institución se encuentra en la etapa 3 del sistema de seguridad de la información, contenido en el documento técnico de Dipres 2013 y que durante esta etapa ha debido implementar un programa de trabajo, de acuerdo al Plan General de Seguridad de la Información, registrando y controlando las actividades comprometidas y desarrolladas.

Finalmente señalar, que en atención a los expuesto en los numerales y párrafos anteriores, esta Superintendencia ha adoptado íntegramente los procederes informados y, que aquellas materias que por su volumen y característica no es posible abordar en forma inmediata se han incorporado en el calendario de actividades que debe desarrollarse e implementarse en las fechas señaladas en el cuerpo de este documento.

Saluda atentamente a Ud.,

SUPERINTENDENCIA DE ELECTRICIDAD Y COMBUSTIBLES - SUPERINTENDENTE -

Luis Ávila Bravo
Superintendente de Electricidad y Combustibles

SUPERINTENDENCIA DE ELECTRICIDAD Y COMBUSTIBLES ★ DAF

CMC/JGD/frr/lcm

Distribución:
Destinatario
- DAD
- DI
- Oficina de Partes ()

Caso Times:_____ /