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

REF. N° 225.613/2013
DAA N° 2.918/2014

REMITE INFORME DE SEGUIMIENTO QUE INDICA.

SEC
OFICINA DE PARTES
15 / SEPTIEMBRE / 2014
14614

SANTIAGO, 11 SET 14 *70950

Adjunto remito a Ud., para su conocimiento y fines pertinentes, copia del Informe de Seguimiento al Informe Final N° 2, de 2013, debidamente aprobado, sobre auditoría de sistemas, efectuada en la Superintendencia de Electricidad y Combustibles, SEC.

Saluda atentamente a Ud.,

POR ORDEN DEL CONTRALOR GENERAL
GLORIA BRIONES NEIRA
Jefe (S) División de Auditoría Administrativa

A LA SEÑORA
JEFA DE AUDITORÍA INTERNA
SUPERINTENDENCIA DE ELECTRICIDAD Y COMBUSTIBLES
PRESENTE

RTE
ANTECED

DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
UNIDAD DE SEGUIMIENTO

INFORME DE SEGUIMIENTO

Superintendencia de Electricidad y Combustibles

Número de Informe: 2/2013
11 de septiembre de 2014

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

USEG N° 98/2014
REF N° 225.613/2013

SEGUIMIENTO AL INFORME FINAL N° 2, DE 2013, SOBRE AUDITORÍA DE SISTEMAS EFECTUADA EN LA SUPERINTENDENCIA DE ELECTRICIDAD Y COMBUSTIBLES.

SANTIAGO, 11 SET. 2014

De acuerdo a las facultades establecidas en la ley N° 10.336, de Organización y Atribuciones de la Contraloría General de la República, se realizó el seguimiento a las observaciones contenidas en el Informe Final N° 2, de 2013, sobre auditoría de sistemas efectuada en la Superintendencia de Electricidad y Combustibles, en adelante e indistintamente SEC, con la finalidad de verificar el cumplimiento de las medidas requeridas por este Organismo de Control. El funcionario que ejecutó esta fiscalización fue el Sr. Rodrigo Ramírez Tapia.

El proceso de seguimiento consideró la respuesta del servicio al citado Informe Final N° 2, de 2013, remitida a este Ente Contralor mediante el oficio N° 10.251, de 2013.

Los antecedentes aportados fueron analizados y complementados con las validaciones correspondientes en el ente fiscalizado, a fin de comprobar las acciones correctivas implementadas, arrojando los resultados que en cada caso se indican.

Contralor General de la República

AL SEÑOR
RAMIRO MENDOZA ZÚÑIGA
CONTRALOR GENERAL DE LA REPÚBLICA
PRESENTE

1. OBSERVACIONES QUE SE SUBSANAN

N° OBSERVACIÓN	DESCRIPCIÓN DE LA OBSERVACIÓN	RESPUESTA DE LA ENTIDAD	ANÁLISIS DE LA RESPUESTA Y VERIFICACIONES REALIZADAS	CONCLUSIÓN
III – 1 – Decreto N° 83, de 2004, del MINSEGPRES	a) Se detectó que la Política de Seguridad Institucional no especifica los mecanismos de difusión de los contenidos al interior de la organización, lo que vulnera el artículo 11, del citado decreto N° 83. Del mismo modo, evaluadas las instrucciones relativas al consumo de alimentos, bebidas y tabaco en las cercanías de sistemas informáticos, así como las condiciones climatológicas y ambientales que pueden afectar a estos o entornos cercanos, se comprobó que no se impartían ni publicitaban, infringiendo lo estipulado por el artículo 18 del citado cuerpo reglamentario.	Al respecto, el servicio señaló que efectuó la modificación a la Política de Seguridad de acuerdo a lo solicitado mediante la resolución exenta N° 1.526, de 2 de julio de 2013, en la que se especifica que la SEC desarrolla actividades periódicas de difusión y entrenamiento de políticas de seguridad de la información a los distintos estamentos de su personal. Agregó, que tales políticas se publican en intranet institucional, y se realizan charlas semestrales a través de las cuales se capacita al personal de la institución respecto de esas materias. Adicionó, que durante el año 2013 se llevó a cabo la difusión de esta y otras políticas y procedimientos relacionados con la seguridad de información, a través de correo electrónico enviado por la unidad de comunicaciones, el 19 de agosto de 2013, siendo publicado en la intranet del servicio en la misma fecha, poniendo a disposición el links para la descarga de documentos.	Se acreditó la actualización de la aludida Política de Seguridad Institucional, a través del cual se detallan cada uno de los contenidos específicos vinculados con esa materia, comprobando además dentro de dicho procedimiento, las instrucciones dispuestas para dar cumplimiento sobre el consumo de alimentos, bebidas y tabaco dentro de sus dependencias, entre otras.	Considerando que el ente fiscalizador adoptó las medidas requeridas para normalizar lo detectado, este se da por subsanado.
	b) Se comprobó que las instrucciones impartidas no incluían la indicación de cambiar las contraseñas, cuando hayan indicios de una brecha en la seguridad, así como la recomendación de elegir contraseñas que sean fáciles de recordar, que contengan letras, mayúsculas, dígitos, y caracteres de puntuación, que no estén basados en elementos obvios o de fácil deducción, trasgrediendo lo expuesto en el artículo 28 del aludido decreto.	El servicio indicó que se realizó la modificación de la resolución exenta N° 1.526, de 2 de julio de 2013, de acuerdo a lo solicitado, especificando las recomendaciones para la generación y cuidado de las contraseñas.	Por intermedio del aludido acto administrativo, se advirtió la actualización de las políticas de seguridad de la institución, ratificando las nuevas instrucciones relacionadas con la utilización de contraseñas de sus usuarios, entre las cuales se describen las siguientes: No escribir en papeles de fácil acceso; No habilitar la opción "Recordar clave de este equipo"; No enviarla por correo, entre otras.	Atendido a que el ente fiscalizado dispuso de medidas que apuntan a la regularización de los hechos objetados, estos se dan por subsanados.
	c) Respecto a la revisión efectuada sobre las buenas prácticas implantadas en el servicio, se constató que no son promovidas para reducir el riesgo de acceso no autorizado a documentos electrónicos o sistemas informáticos, vulnerando lo estipulado por el artículo 31 del mencionado texto normativo.	Sobre este punto, la entidad auditada respondió que formalizó la política específica de control de acceso de información, a través de la resolución exenta N° 809, de 3 de abril de 2013, en donde se precisan además, los deberes de los usuarios en cuanto al control de acceso a la información; acceso a instalaciones de procesamiento de información; documentos electrónicos; redes y sistemas informáticos; lo que fue publicado en la intranet y enviado a los funcionarios vía correo institucional.	La citada resolución exenta, da cuenta de las instrucciones impartidas por la institución sobre estas materias, evidenciándose además que en la información complementaria, se ejecutaron las modificaciones para acceder a los sistemas informáticos del servicio.	

N° OBSERVACIÓN	DESCRIPCIÓN DE LA OBSERVACIÓN	RESPUESTA DE LA ENTIDAD	ANÁLISIS DE LA RESPUESTA Y VERIFICACIONES REALIZADAS	CONCLUSIÓN
III – 1 – Decreto N° 83, de 2004, del MINSEGPRES	d) En relación con el análisis realizado sobre la coordinación con las autoridades de emergencia, como policía, bomberos, autoridades directivas, entre otros, se advirtió la inexistencia de un plan que regulara las comunicaciones entre la institución y las autoridades aludidas, infringiendo lo indicado por el artículo 35 del decreto ya citado.	En su respuesta, la superintendencia señaló que dispuso del "PLAN DE EMERGENCIA Y EVACUACIÓN SEC", el que se encuentra en cada una de una de las sedes de la entidad, es decir, en Direcciones Regionales, Oficinas Provinciales y Oficinas del Nivel Central. Añadió, que estos documentos se encuentran publicados en la intranet institucional, http://intranet2.sec.cl/prevencion-de-riesgos/. A modo de ejemplo, adjuntó el Plan de Emergencia de la Oficina Central.	Se comprobó a través de la página institucional de la entidad, la difusión de los respectivos planes de emergencia y evacuación.	En virtud de lo expuesto se subsana la observación formulada.
	f) En el caso particular de la acreditación de las referencias del personal que posee acceso a los equipos de procesamiento de datos y a los que manipulan información sensible, se detectó que dicho proceso no se efectúa.	La SEC manifestó en su oficio de respuesta que incluyó en los contratos de proveedores adjudicados de procesos licitatorios, el siguiente texto, "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".	Al respecto, es dable indicar que las mencionadas medidas fueron corroboradas mediante los referidos contratos de proveedores licitados por el servicio durante el primer semestre del año 2014.	Las acciones adoptadas permiten dar por subsanadas las objeciones.
	i) Analizadas las cláusulas en los contratos de personal, se verificó la inexistencia de aquellas que especifiquen sanciones, en el caso que el personal intente accesar sin autorización en los sistemas informáticos, contraviniendo lo estipulado en la letra g) del artículo 37, del citado decreto. Esta situación fue corroborada mediante memorándum S/N, de 17 de diciembre de 2012, por el Jefe de la Unidad de Personal.	La Superintendencia de Electricidad y Combustibles expuso en su contestación que a partir del mes de abril del año 2013, se incorporó la cláusula séptima en los convenios a honorarios, donde se establece la confidencialidad en el uso de información, la obligación de acceder sólo a los sistemas a los que se encuentra autorizado y la sanción en caso de incumplimiento. Añadió, que a partir de los nombramientos del mes de octubre del 2013, se agregó una declaración jurada a los documentos que deben completar los funcionarios, cuando se incorporan a esa repartición.	Sobre el particular, se corroboraron las modificaciones realizadas tanto en los contratos a honorarios, así como también se tuvieron a la vista las declaraciones juradas para los casos de contratación de su personal, confirmando en ellos la cláusula que estipula la confidencialidad del uso de la información.	

2. OBSERVACIONES QUE SE MANTIENEN

N° OBSERVACIÓN	DESCRIPCIÓN DE LA OBSERVACIÓN	RESPUESTA DE LA ENTIDAD	ANÁLISIS DE LA RESPUESTA Y VERIFICACIONES REALIZADAS	CONCLUSIÓN	ACCIÓN DERIVADA
III – 1 – Decreto N° 83, de 2004, del MINSEGPRES	e) Para comprobar la validez de la política de seguridad, el costo e impacto de los controles en la eficiencia del negocio y los cambios de tecnología, se acreditó que el cronograma de revisiones periódicas no indica que se evaluará su efectividad, contraviniendo lo establecido en la letra a), del artículo 37 del mismo cuerpo normativo.	Sobre el particular, la entidad comunicó que realizó modificaciones a la política de seguridad, aprobadas por la resolución exenta N° 1.526, 20 de julio de 2013, especificándose que dicha política será revisada y evaluada anualmente, lo que será verificado en el mes de noviembre de cada año, desde su aprobación por el Comité de Seguridad de la Información de la SEC, quien además propondrá los ajustes pertinentes al superintendente, si correspondiese.	En relación a la materia, cabe consignar que si bien se corroboró que la SEC actualizó su política de seguridad, es pertinente manifestar que su revisión y actualización, no ha sido llevada a cabo por la entidad de acuerdo al lineamiento definido, manteniéndose esta evaluación pendiente a la fecha de este seguimiento.	Considerando lo expuesto, la observación se mantiene.	La SEC deberá dar cumplimiento a lo dispuesto en sus políticas de seguridad de la información, acciones que serán verificadas en una futura auditoría que realice este Órgano Superior de Control.
	h) En atención a la validación efectuada sobre los equipos computacionales que se usan fuera de la organización, se constató que estos, no se encuentran asegurados por compañías del rubro.	En cuanto a esta materia, es preciso mencionar que mediante el memorándum N° 892.118, de 21 de mayo de 2012, el Subdepartamento de Administración de la SEC, informó 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, por tanto, en tales circunstancias se reitera el criterio utilizado en el memorando N° 826.338, de fecha 21 de marzo de 2013, en orden a no contratar una póliza de seguro.	Al respecto, y tal como lo ha comunicado la autoridad de la repartición, los aludidos equipos computacionales, continúan sin estar cubiertos por una empresa aseguradora.	Atendido lo anterior, la observación se mantiene.	La entidad fiscalizada deberá adoptar las medidas necesarias que permitan que sus bienes y equipos computacionales estén cubiertos de los riesgos de pérdida o extravío, lo que será comprobado en una futura fiscalización que efectúe este Organismo Contralor.
	j) En el análisis realizado al Plan de Contingencia, se comprobó que este no incluye la identificación de los eventos que pueden causar interrupciones a los procesos del negocio, ni una valorización del riesgo para determinar el impacto de las interrupciones a los procesos críticos, asimismo, este no se encuentra aprobado por la dirección, vulnerando lo establecido en la letra i), del referido artículo 37.	La institución auditada expuso en su oficio de respuesta que el departamento de informática ejecutó un cronograma de actividades las que se detallan como sigue: En noviembre 2013, efectuarán una revisión y actualización del actual Plan de Contingencia; en diciembre 2013, realizarán la 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. Finalmente, comentó que en abril de 2014, hará una simulación controlada en la ejecución de los planes de contingencia y ajustes si correspondiere.	En lo concerniente a la aplicación de estas medidas, se constató que estas no han sido llevadas a cabo por parte del ente fiscalizado.	En razón de lo argumentado, la observación se debe mantener.	La aplicación de estas medidas, será corroborado en una futura fiscalización que realice esta Contraloría General.

N° OBSERVACIÓN	DESCRIPCIÓN DE LA OBSERVACIÓN	RESPUESTA DE LA ENTIDAD	ANÁLISIS DE LA RESPUESTA Y VERIFICACIONES REALIZADAS	CONCLUSIÓN	ACCIÓN DERIVADA
III – 2 - Decreto N° 93, de 2006, del MINSEGPRES	En relación con el procedimiento que regula la desvinculación de los funcionarios del servicio, se detectó que al cesar un usuario de sus funciones, no existe una configuración del servidor de correo que rechace automáticamente los mensajes electrónicos dirigidos a la casilla institucional personal que haya estado asignada, ni un mensaje de aviso para que el recurrente disponga de una o mas casillas electrónicas alternativas a las cuales redirigirse, infringiendo con ello lo señalado en el articulo 9° del referido decreto.	La entidad auditada reiteró en su respuesta que realizará las modificaciones al procedimiento de rebaja de los usuarios de los sistemas de información de la SEC, incluyendo actividades para la reconfiguración de las cuentas de correos de los funcionarios desvinculados. Añadió, que la implementación en el servidor de correo electrónico institucional será desarrollada por personal de la SEC, el que será publicado en la intranet y difundido a través de correo electrónico, teniendo como plazo el mes de diciembre 2013.	Sobre el particular, es pertinente manifestar que esa superintendencia a la fecha del presente seguimiento no ha llevado a cabo lo comprometido.	En virtud de lo argumentado, la observación formulada se mantiene.	Las acciones adoptadas para dar cumplimiento a lo dispuesto en el citado artículo 9° del decreto N° 93, de 2006, serán verificadas en una futura fiscalización que este Organismo Contralor realice sobre la materia.
III – 3 - Decreto N° 100, de 2006, del MINSEGPRES	En cuanto a las pruebas practicadas sobre la estructura de las hojas de estilo en cascada y del sitio Web, se advirtió que no se valida el código de despliegue utilizado en el mismo, transgrediendo así lo indicado en el artículo 5°, del aludido decreto. Lo anterior da cuenta además de una infracción a los artículos 61 y 64 de la ley N° 18.834, sobre Estatuto Administrativo, en lo relativo a la obligación de los funcionarios de dar cumplimiento a la normativa y la obligación de las jefaturas de ejercer un control jerárquico permanente ligado al personal de su dependencia, en lo que dice relación con el cumplimiento de planes, programas y normas. Al respecto, la autoridad del servicio informó que realizó una revisión del código del sitio Web, usando como validador el consignado en el artículo 5° del decreto N° 100 precitado, www.w3.org. Del mismo modo, agregó que a partir de los errores identificados en ese proceso, hizo los ajustes y modificaciones en la codificación, evidenciando en su respuesta que el chequeo de los validadores de CSS y HTML, generaron resultados satisfactorios. Además, precisó que realizaría una evaluación completa del sitio Web institucional en lo referente a los estándares W3C, fijando como plazo para estas actividades el 30 de mayo de 2013.	La superintendencia manifestó en su respuesta que adoptó una serie de medidas tales como la identificación y clasificación de errores sobre la estructura de las hojas de estilo en cascada, y del sitio Web, en el período octubre a diciembre 2013, a su vez, efectuó la corrección de errores del período enero - abril 2014, y adicionalmente instruyó a la Unidad de Comunicaciones de la SEC que todas las páginas nuevas que se agreguen al sitio, deberán construirse bajo el estándar especificado en la letra a) del referido decreto N° 100, de 2006. Asimismo, hace presente que la institución se encuentra en la etapa 3 del sistema de seguridad de la información, contenida 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, señaló que la superintendencia ha considerado íntegramente los procederes informados y, que aquellas materias que por su volumen y característica no es posible abordar en forma inmediata, se incorporaron en el calendario de actividades a desarrollar e implementarse en fechas posteriores.	Analizados los antecedentes proporcionados, se desprende que si bien la institución ha revisado y materializado las pruebas respectivas sobre la materia con las áreas técnicas pertinentes, se comprobó que el sitio Web institucional, aún presenta inconsistencias, como las detectadas en el Informe Final N° 2, de este origen, lo que fue ratificado además por intermedio del validador Web http://validador.w3.org/, el cual arrojó como resultado una cantidad de 11 errores.	En atención a lo expuesto, la observación se mantiene.	El estricto acatamiento del decreto N° 100, de 2006, del MINSEGPRES, será corroborado en una próxima auditoría que ejecute esta Contraloría General.

CONCLUSIONES

En mérito de lo expuesto, cabe concluir que la Superintendencia de Electricidad y Combustibles, realizó gestiones que permitieron subsanar las observaciones contenidas en el cuadro N° 1 del presente informe.

No obstante lo anterior, se mantienen las situaciones informadas en el cuadro N° 2, con las acciones derivadas que en cada caso se indican.

Transcríbase al Ministro de Energía, al Superintendente de Electricidad y Combustible, a la jefa de Auditoría Interna de esa misma repartición, y al Jefe de la Unidad Técnica de Control Externo de la División de Auditoría Administrativa de esta Contraloría General.

Saluda atentamente a Ud.,

GLORIA BRIONES NEIRA
Jefe (S) División de Auditoría Administrativa

www.contraloria.cl