

CONTRALORÍA GENERAL DE LA REPÚBLICA
División de Auditoría Administrativa
Área Administración General y Defensa Nacional

Informe Final
Presidencia de la República



Fecha : 14 de abril de 2011
N° Informe : 7/2011



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

DAA. N° 606 /2011

REMITE INFORME FINAL N° 7 DE 2011,
SOBRE AUDITORÍA DE SISTEMAS EN LA
PRESIDENCIA DE LA REPÚBLICA.

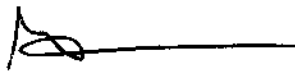
SANTIAGO, 14. ABR 11 *022909

Cumplo con enviar a Ud. para su conocimiento y fines pertinentes, copia del Informe Final N° 7 de 2011, con el resultado de la auditoría de sistemas practicada en la Presidencia de la República.

Sobre el particular, corresponde que ese Servicio implemente las medidas señaladas, cuya efectividad, conforme a las políticas de esta Contraloría General sobre seguimiento de los programas de fiscalización, se comprobarán en una próxima visita a la entidad.

Saluda atentamente a Ud.,




Por Orden del Contralor General
MARÍA ISABEL CARRIL CABALLERO
Abogado Jefe
División de Auditoría Administrativa

AL SEÑOR
DIRECTOR ADMINISTRATIVO
PRESIDENCIA DE LA REPÚBLICA
PRESENTE

Ref. N°165.735 / 2011





CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

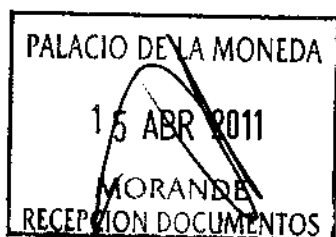
DAA. N°607 /2011

REMITE INFORME FINAL N° 7 DE 2011,
SOBRE AUDITORÍA DE SISTEMAS EN LA
PRESIDENCIA DE LA REPÚBLICA.

SANTIAGO, 14. ABR 11 *022910

Cumplo con enviar a Ud. para su conocimiento, copia del Informe Final N° 7, de 2011, con el resultado de la auditoría de sistemas efectuada en la Presidencia de la República.

Saluda atentamente a Ud.,



Por Orden del Contralor General
MARÍA ISABEL CARRIL CABALLERO
Abogado Jefe
División de Auditoría Administrativa

AL SEÑOR
JEFE DE UNIDAD DE AUDITORÍA INTERNA
PRESIDENCIA DE LA REPÚBLICA
PRESENTE
Ref. N° 165.735/ 2011





CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

PMET: 13.154

INFORME FINAL N° 7 DE 2011 SOBRE
AUDITORÍA DE SISTEMAS EN LA
PRESIDENCIA DE LA REPÚBLICA.

SANTIAGO, 14 ABR. 2011

En cumplimiento del plan de fiscalización de esta Contraloría General para el año 2010, y de acuerdo con las facultades establecidas en la ley N° 10.336, Orgánica de esta Contraloría General, funcionarios de este Organismo de Control se constituyeron en la Presidencia de la República, para efectuar una Auditoría de Sistemas, con el objetivo de revisar, entre otros aspectos, la seguridad informática.

OBJETIVO

La auditoría tuvo por finalidad examinar y evaluar aspectos que se relacionan con las políticas, normas, prácticas y procedimientos de control vinculados con los Sistemas de Tecnologías de la Información y las Comunicaciones, TIC, de la Presidencia de la República.

METODOLOGÍA

La revisión fue practicada en conformidad con las principales normas y procedimientos aceptados por esta Entidad Fiscalizadora, incluyendo pruebas de validación y otros medios técnicos considerados necesarios en las circunstancias.

COBERTURA

El examen comprendió la revisión de normativas de las TIC, de conformidad con lo dispuesto en los decretos supremos del Ministerio Secretaría General de la Presidencia, MINSEGPRES, referidas a las siguientes normas técnicas:

- N° 77, de 2004: Norma técnica sobre Eficiencia de las Comunicaciones Electrónicas entre Órganos de la Administración del Estado y entre éstos y los ciudadanos.

A LA SEÑORA
JEFA DE LA DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
PRESENTE
RCA



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

- N° 81, de 2004: Norma técnica para los órganos de la Administración del Estado sobre interoperabilidad del documento electrónico.
- N° 83, de 2004: Norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad del documento electrónico.
- N° 93, de 2006: Norma técnica para minimizar la recepción de mensajes electrónicos masivos no deseados en las casillas electrónicas de los órganos de la Administración del Estado y de sus funcionarios.
- N° 100, de 2006: Norma técnica para el desarrollo de sitios web de los órganos de la Administración del Estado.

Por otro lado, se procedió a realizar una evaluación de dos sistemas informáticos que se encuentran operativos en la Presidencia de la República: el Sistema Integral de Gestión Administrativa, SIGA, y el Sistema Subvenciones Presidenciales.

Resultado del examen

Mediante oficio N° 11.251, del 23 de febrero de 2011, esta Contraloría General remitió a la Presidencia de la República el Preinforme de Observaciones N° 7, de 2011, con el objeto que informara respecto de las situaciones observadas, dándose respuesta a éste a través del oficio confidencial N° 6, del mismo año, cuyo análisis y antecedentes aportados sirvieron de base para la elaboración del presente Informe Final.

I. ANTECEDENTES GENERALES

La misión de la Presidencia de la República es apoyar al Presidente de la República¹. La Dirección Administrativa de esta Entidad tiene por función apoyar en todo momento y lugar al Primer Mandatario, brindando todo el apoyo logístico necesario, administrando de manera eficiente y eficaz todos los recursos a su disposición. También es responsable del mantenimiento del Palacio de la Moneda y del Palacio de Cerro Castillo.

La Subdirección Administrativa es una dependencia de la Dirección Administrativa que apoya la labor del Director Administrativo. Está constituida por diferentes departamentos, subdepartamentos y secciones. Entre éstos, se encuentra el Departamento de Informática, DI, encargado de contribuir a "la mejora continua de la gestión de la Presidencia de la República mediante la incorporación, adaptación y operación de Tecnologías de Información y Comunicaciones." Administra todo lo referente a las Tecnologías de Información y Comunicaciones, TIC (redes, datos, software y hardware).

Contralor General
de la República

¹ Resolución exenta N° 3663, del 5 de noviembre de 2010, de la Presidencia de la República, Dirección Administrativa.



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

II. EL DEPARTAMENTO DE INFORMÁTICA DE LA PRESIDENCIA DE LA REPÚBLICA

1. Organización

El Departamento de Informática opera con tres secciones: Seguridad y Servicios Críticos; Desarrollo y Mantenimiento de Sistemas; y Operaciones y Sistemas. Anexo N° 1.

2. Redes

La Presidencia posee una red de área local LAN Ethernet, con dos conexiones a internet.

3. Servidores

El Servicio tiene una sala de servidores con cinco racks, entre los cuales se distribuyen 80 equipos, divididos en organizadores de fibra óptica, Transceivers², Routers, RPS³ (UPS), firewalls y servidores. De estos últimos, existen 26 equipos, de los cuales 24 son de marca Dell, uno NEC y uno Sunshine según se consigna en el Anexo N°2.

El Departamento de Informática dispone también de "servidores virtuales" que se encuentran en máquinas con procesadores Intel Xeon E5410 de 2,33Ghz, que entregan distintos servicios como se detalla en el Anexo N°3.

4. Aplicaciones

Las principales aplicaciones básicas de productividad en la red de la Presidencia se encuentran en la siguiente tabla:

Aplicación	Software
Respaldo	BackupExec 2010
Correo	Exchange 2007
Base Datos	SQL 2008
Antivirus	Suite TrendMicro
VmWare	VsPHERE Enterprise

5. Hardware y software básico de oficina

La resolución exenta N° 2181, del 20 de noviembre de 2008, de la Dirección Administrativa, aprobó el contrato con la empresa Net Now Tecnología y Computación S.A. para el arrendamiento de equipos computacionales. Dicho arriendo considera 380 computadores personales y 20 notebooks. El contrato fue suscrito el 1 de octubre de 2008 con un plazo de duración de 24 meses y por un valor total de 16.329,47 Unidades de Fomento, U.F., con un canon de arriendo mensual de 680,40 U.F. Los equipos tienen instalado el sistema

² Transmisor- Receptor donde ambas funciones comparten gran parte de los circuitos.

³ Redundant Power system



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

operativo Windows XP Pro, tal como precisa la Dirección Administrativa de la Presidencia en su respuesta, y la suite de oficina de Microsoft Office 2003.

Asimismo, la resolución exenta N° 737, de 22 de febrero de 2010, de la Dirección Administrativa, autorizó la contratación directa con la misma empresa para el arriendo de 45 computadores durante doce meses, desde el 2 de febrero de 2010 hasta el 5 de febrero de 2011, y de otros 14 computadores desde el 23 de octubre de 2009 hasta el 31 de diciembre de 2010, por un valor de UF2.021,05.

Entre otros software que tiene el Servicio se encuentran: Visual C++, MS Visual Studio 2008 Profesional, MS Visio MUI, MS SQL server, entre otros.

6. Software (CORE BUSSINES)

El Departamento de Informática de la Presidencia de la República dispone de un software desarrollado específicamente para cubrir las necesidades particulares del Servicio. La mayoría de este software es desarrollado por el mismo. Igualmente, la Entidad auditada cuenta con desarrollos externos, como son el software DEXON, los sistemas de Control de Asistencia, ASISCAD, y FINGERACCES. EL detalle de cada sistema se encuentra en el Anexo N°4, con información proporcionada por el Departamento de Informática.

7. Seguridad de la red

En conjunto con personal del Departamento de Informática, se revisó el sistema de seguridad de la red de la Presidencia. Ésta cuenta con zona desmilitarizada, cortafuegos, anti virus y anti Spam. El tráfico de las páginas web es monitoreado mediante Google Analytic. Los log de los Firewall e IPS son monitoreados por un equipo Cisco MARS, que es el que correlaciona los eventos.

Esta Contraloría General revisó las medidas de seguridad de la red de computadores que utiliza la Presidencia, la cual se encuentra conectada a dos redes WAN, que le dan acceso a Internet. La principal es una conexión MPLS⁴ brindada por la Empresa Nacional de Comunicaciones S.A. (Entel). Este servicio está avalado por el contrato firmado el 15 de noviembre de 2008, con una duración de 36 meses prorrogables automáticamente, por períodos de un año. La otra conexión es mediante la red del Estado.

La arquitectura de la red incluye una DMZ (Zona desmilitarizada) con gateway de correo sin acceso a la base de clientes de correo. Hay un FireWall Cisco con varios firewall virtuales. La red está segmentada con el servicio de un router central en subredes. También usa Wi-Fi con WPA (Wi-Fi Protected acces) para seguridad y autenticación de la conexión inalámbrica, además de identificación por MAC⁵. Se utiliza también SHA1 (Secure hash algorithm: funciones de hash para criptografía).

⁴ MPLS: Multi Protocol Label Switching: "Es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP". (http://es.wikipedia.org/wiki/Multiprotocol_Label_Switching)

⁵ Media Access Control.



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

8. Sistemas a auditar

El Departamento de Informática de la Presidencia de la República administra o alberga en sus servidores una serie de sistemas informáticos, ver detalle en el Anexo N°4, ya citado. De estos sistemas, se seleccionaron dos para ser evaluados: el sistema SIGA-Personal-Remuneraciones y el Sistema de Subvenciones Presidenciales.

III. INCUMPLIMIENTO DE NORMATIVA APLICABLE

La revisión se limitó a verificar el cumplimiento de los decretos supremos del Ministerio Secretaría General de la Presidencia, MINSEGPRES, relacionados con el ambiente TI, antes señalados.

En su respuesta el Servicio señala que “un número significativo de las observaciones” fueron incorporadas al Plan Anual de Proyectos 2011, situación que será revisada en una futura visita de seguimiento.

1. Decreto supremo N° 77, de 2004, del MINSEGPRES

En lo referente a las comunicaciones electrónicas, no se cumple con lo consignado en el artículo 7 de la mencionada normativa. Es decir, al realizar cierres mensuales de todos los registros diarios acumulados durante el período comprendido entre el último cierre y el que se realiza, no hay ministro de fe, ni firma electrónica.

El Organismo indica en su respuesta que la designación del citado ministro será considerada en la resolución que aprueba el Plan Anual de Proyectos 2011. Situación que será verificada en la visita de seguimiento.

2. Decreto supremo N° 81, de 2004, del MINSEGPRES

En lo referente al manejo de los documentos electrónicos, el Servicio auditado manifiesta que no maneja documentos en formato XML, agregando que no tiene documentos que requieran firma electrónica. Sin embargo, tiene esquemas referenciados en documentos públicos y de libre acceso, inscritos en la resolución 452 AEM⁶, por lo cual no se da cumplimiento al precitado decreto N° 81.

El Servicio en su respuesta, señala que los esquemas XML ya fueron inscritos en el contexto de los proyectos de interoperabilidad del sistema de Correspondencia de la Ciudadanía con el Presidente, que aún está en fase de desarrollo y prueba, considerándose que la implementación definitiva recién estará operativa el segundo semestre de 2011. Lo que será revisado por parte de esta Entidad de Control en una próxima auditoría.

⁶ Ver archivos “Descripción del XML correspondencia Presidencia 2009-11-19-v1.0.pdf” y “AEM-Informe Foro Inscripción 452.pdf” en el CD con la documentación.



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

3. Decreto supremo N° 83, de 2004, del MINSEGPRES

En lo referente a la seguridad y confidencialidad de los documentos electrónicos, no se da cumplimiento a las obligaciones consignadas en los siguientes artículos:

- Artículo 11: Existe una política de seguridad aprobada el 30 de diciembre de 2010, no obstante, los mecanismos de difusión de ésta son vagos.

En su respuesta, la Entidad examinada señala que contemplan un "programa de alta difusión de la política de seguridad" para la última semana de marzo de 2011.

- Artículo 12: La política de seguridad no designa explícitamente a un encargado de seguridad.

El Servicio en su respuesta, identifica el encargado de seguridad, el cual fue nombrado por la resolución exenta N°2.630, de 30 de julio de 2010, de la misma Entidad. Los antecedentes puestos a disposición de este Organismo Fiscalizador permiten dar por superada la observación.

- Artículo 13: No se clasifican ni etiquetan los documentos electrónicos y sistemas informáticos para indicar la necesidad, prioridad y grado de protección.

Al respecto, el Servicio auditado precisa que durante el año 2010 se aplicaron estándares de alta prioridad a todos los sistemas informáticos, sin distinción. No obstante, se compromete a que en el transcurso del primer semestre de 2011, implementará un sistema de clasificación y etiquetado.

- Artículo 17: No existe un procedimiento formal o política de seguridad física.

La Presidencia de la República manifiesta que tiene proyectado formalizar este procedimiento antes del término del primer semestre del año 2011.

- Artículo 20: No existen instrucciones formales del Jefe de Servicio con respecto a la prohibición de instalación de software no autorizado, documentos y archivos guardados en el computador.

En relación a este punto, el Servicio objeto de la presente auditoría señala que en la política de seguridad y en la ficha de recepción de equipos informáticos del mismo, efectivamente, se considera esa prohibición. De acuerdo a los antecedentes complementarios puestos a disposición de esta Entidad de Control, la observación se da por superada.

- Artículo 24: No existe un sitio externo de respaldo por lo que no existe política de acceso a éste.

El Servicio informa que en coordinación con el Ministerio del Interior, se encuentran diseñando una solución para sitios de



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

contingencia, respecto a lo cual estima que contará con una solución durante el segundo semestre de 2011.

- Artículo 26: Se formatean los equipos antes de ser dados de baja solo para el "personal relevante", no para todos los equipos.

Al respecto, el Servicio en su respuesta señala que a partir de la última semana de marzo de 2011, el proceso de renovación de PC contempla el formateo de equipos, junto con la proyectada renovación de equipos, adjuntando el "Procedimiento de formateo de discos duros". Sin embargo, en este documento se describe brevemente el procedimiento técnico para realizar el proceso, pero no se hace mención alguna a los aspectos administrativos y prácticos de la realización del mismo. A modo de ejemplo, no menciona quién o quiénes son los responsables de realizarlo, tampoco indica cómo se asegura que todo equipo que deje de ser utilizado en la Presidencia siga, forzosamente, este procedimiento de borrado. Lo anterior, entre otros aspectos necesarios, no permite considerar dicho documento como un respaldo suficiente como para dar por superada esta observación.

- Artículo 28: Las instrucciones al personal no incluyen la indicación de cambiar las contraseñas cuando hayan indicios de un posible compromiso del identificador o del sistema. Sin embargo, éstas indican que se debe dar aviso al Director del Departamento de Informática. En otro aspecto de este artículo sólo se dispone que las claves tengan ocho caracteres y no que incluyan mayúsculas minúsculas, dígitos y caracteres especiales, ni tampoco que contemplen datos obvios como la fecha de nacimiento, el RUT, entre otros.

En su respuesta el Servicio manifiesta que "...en el acta de entrega de equipos se entregarán las instrucciones..." a las que se refiere este artículo, durante la última semana de marzo, cuando habrá un cambio masivo de equipos y de proveedor de éstos. No obstante, no se hace referencia a la adopción de una política permanente, más amplia, que incluya por ejemplo, la difusión permanente o la entrega de estas instrucciones a todo nuevo personal que se incorpore a la Presidencia. Por lo tanto, la observación se mantiene.

- Artículo 31: No se promueven buenas prácticas para reducir el riesgo de acceso no autorizado a documentos electrónicos o sistemas informáticos, como por ejemplo, las de pantalla limpia.

El Servicio se compromete a implementar lo señalado en este punto a partir de marzo de 2011.

- Artículo 33: Inexistencia de procedimientos formales de autorización para determinar quién tiene permitido acceder a que redes y servicios de red.

El Servicio responde que esto estaría operativo antes del término del primer semestre de 2011.

- Artículo 35: Falta de un plan de contingencia para asegurar la continuidad de operaciones críticas para la Institución.



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

El Servicio, según lo señalado en su respuesta, tiene proyectado formalizar un procedimiento de contingencia, antes del término del primer semestre de 2011.

- Artículo 37 a: El cronograma de revisiones periódicas no indica explícitamente que se evaluará la efectividad de la política, el costo e impacto de los controles en la eficiencia del negocio y los cambios de tecnología. La política de seguridad no incluye procedimientos de delegación de autoridad para ejecutar acciones de emergencia en los sistemas y los procedimientos correspondientes.

Al respecto, la Presidencia indica que pretende tener solucionado este punto antes del término del primer semestre de 2011.

- Artículo 37 c: No existen procedimientos para el etiquetado y la manipulación de los documentos electrónicos.

De acuerdo a lo señalado por la Entidad, en el transcurso del primer semestre de 2011 se implementará un sistema de clasificación y etiquetado.

- Artículo 37 d: Al personal que tiene acceso a los equipos de procesamiento de la información y a los que manipulan información sensible, no se les verifica sus referencias comerciales, ni las personales. El personal del Servicio no ha firmado un acuerdo de confidencialidad o de no divulgación de información sensible.

La Presidencia responde que esto se contrapone a lo dispuesto en el artículo 12 del Estatuto Administrativo, ley N° 18.834 y a la jurisprudencia contenida en el dictamen N° 75.467, de 2010, de esta Contraloría General. Agrega, que sólo los "contratos con terceros" establecen responsabilidades y derechos del empleado en relación a los derechos de propiedad y respecto a la protección de los datos y de la información.

Sobre el particular, corresponde precisar que si bien la autoridad no puede imponer condiciones para el desempeño de un cargo público, que no se encuentren previstas en la Constitución Política o en las leyes, toda vez que, de hacerlo vulneraría el principio de juridicidad, acorde lo manifestado en dictámenes N° 15.329, de 2008 y 72.866 de 2009, se levanta lo observado, sin perjuicio de manifestar que en resguardo de los bienes o cierta información específica, la Administración debe adoptar las medidas para su debida protección.

- Artículo 37 e: Los equipos que se usan fuera de la organización (como notebook u otro elemento) no tienen cobertura de seguros de protección. Las visitas a las instalaciones sensibles y de procesamiento de información no firman un compromiso de no divulgación, ni se les informa de las restricciones y requisitos de seguridad y de los procedimientos de emergencia del área. El personal de las instalaciones sensibles y de procesamiento de información no usa identificación visible.



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

El Servicio en su respuesta manifiesta que para el presupuesto del año 2012, verá la factibilidad de contratar seguros para proteger a los equipos en uso fuera de los recintos de la institución. Asimismo, indica la existencia de un documento de no divulgación para quienes entren al data center, no obstante, en pruebas realizadas por el equipo auditor, la firma de éste no fue requerida, no cumpliéndose con el objetivo del documento. Por ende, la observación se mantiene hasta que se compruebe en una próxima visita de seguimiento, el efectivo cumplimiento de la obligación consignada en el artículo 33, letra a), del decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia.

- Artículo 37 f: No existe un registro formal de los cambios significativos realizados a las instalaciones y sistemas de procesamiento de información del Servicio. Además, se constató la inexistencia de un informe de la evaluación del impacto de realizar tales modificaciones, de un procedimiento formal de aprobación de las variaciones realizadas a las instalaciones y sistemas de procesamiento de información, y de una comunicación de los detalles de los cambios a realizar, a las personas que se verán afectadas y que participarán en el proceso.

Además, no existe un procedimiento formal que recupere la condición inicial antes de efectuar las modificaciones en caso de presentarse cambios no exitosos. Los dispositivos en desuso que contienen información sensible, no son eliminados por incineración o trituración, o vaciado de los datos mediante otra aplicación dentro del Servicio. Tampoco cuentan con un procedimiento formal que notifique la transmisión, despacho y recepción de información y software, y que defina normas para empaquetar y transmitir información.

Asimismo, no se dispone de una norma oficial, que identifique el servicio Courier a requerir ni las responsabilidades y obligaciones en el contrato con éste, en caso de pérdida de información.

El Servicio se compromete a certificar y formalizar los procedimientos de desarrollo y mantención de sistemas antes del término del año 2011.

A su vez, proporciona antecedentes en relación al sistema Courier, que permiten dar por subsanada esta observación.

- Artículo 37 g: No se incluyen cláusulas en los contratos del personal que especifiquen sanciones si se intenta un acceso no autorizado en los sistemas informáticos.

El Servicio responde que las sanciones para los funcionarios públicos se encuentran en el Título V, artículos 119 y siguientes del Estatuto Administrativo, referido a la responsabilidad administrativa, por lo cual, no sería aceptable esta disposición.

Al respecto, cabe manifestar que no obstante lo dispuesto en el Estatuto Administrativo, en materias de sanciones, a futuro se deben arbitrar las medidas para establecer claramente las sanciones aplicables en caso de infracción al acceso restringido a los sistemas informáticos.

✍



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

- Artículo 37 i: El Servicio no cuenta con un plan de contingencia formal.

Sobre la materia, la Institución fiscalizada se compromete a implementar formalmente un Plan de Contingencia antes del término del primer semestre de 2011.

Siendo ello así, las medidas adoptadas por la Presidencia de la República, para dar cumplimiento a lo observado en relación al presente cuerpo normativo, serán materia de revisión en una futura visita de seguimiento.

4. Decreto supremo N° 93, de 2006, del MINSEGPRES

En cuanto a los correos electrónicos masivos o SPAM, no se da cumplimiento a lo consignado en el artículo 3° del decreto N° 93, de 2006, del Ministerio Secretaría General de la Presidencia, debido a la inexistencia de una guía de protección de casillas electrónicas.

El Servicio manifiesta en su respuesta que se encuentra contemplado en el "Plan Anual de Proyectos 2011" la elaboración de una guía de protección de casillas electrónicas por parte del Departamento de informática, antes del término del primer semestre de 2011, lo cual será motivo de verificación por parte de esta Entidad de Control en una futura visita de seguimiento.

5. Decreto supremo N° 100, de 2006, del MINSEGPRES

En cuanto al cumplimiento de la norma para el desarrollo de sitios web gubernamentales, el del Servicio no se ajusta a todas las recomendaciones contenidas en la Guía de Accesibilidad para Discapacitados en Sitios Web, sin embargo, el Departamento de Informática indicó que está en proceso de cumplirlas. Tampoco cuenta con un plan de contingencia formal.

En relación a lo observado respecto al presente cuerpo normativo, el Servicio señala que se encuentra en proceso de "marcha blanca" la guía antes indicada. Asimismo, indica que se elaborará un plan de contingencia, el que debería estar listo antes del término del primer semestre de 2011, situación que será corroborada en una próxima auditoría.

IV. Sistema SIGA Personal-Remuneraciones

El SIGA es un sistema que tiene dos módulos, el primero llamado Existencias-Abastecimiento, que maneja las existencias y el control del abastecimiento del Servicio, que se encuentra en la etapa de desarrollo, y el segundo, denominado Personal-Remuneraciones, encargado de gestionar al personal y sus remuneraciones, el cual fue revisado por esta Entidad de Control en la presente auditoría.

El último sistema fue desarrollado para registrar los antecedentes del personal de la Presidencia de la República, tales como, datos personales, antecedentes académicos, hoja de vida, datos previsionales, entre otros, para funcionarios de planta, contrata u honorarios. El sistema también calcula la nómina mensual de pago, almacenando los datos necesarios para ello, como el valor de la UF, los tramos de impuestos, y otros parámetros. Adicionalmente, registra las licencias médicas, los atrasos, cargas familiares y otros.



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

1. Listado y Búsqueda

Existen varias opciones de listado, ya sea sólo los datos básicos de los funcionarios⁷, una lista completa con la nómina⁸ o una lista personalizable dinámicamente⁹ por el usuario del sistema. El sistema permite la búsqueda de un funcionario dado su RUT (ver figura N° 1 del Anexo N°5). En este punto, como en los demás, el sistema verifica que sea un RUT válido y si existe o no en la base de datos de forma correcta.

2. Ingreso

Para el ingreso de los datos básicos de un empleado, pestaña "Datos Personales", las validaciones son efectivas: chequea el RUT y que no se repita, además, se cerciora que la fecha de nacimiento no sea posterior al día de ingreso, entre otras validaciones básicas.

Sin embargo, dadas las pruebas realizadas por esta Entidad de Control, se constató que las comprobaciones fallan cuando se trata del ingreso de los bienes. Es así como, en el ambiente de prueba, la Comisión Fiscalizadora ingresó un funcionario con cuatro (4) años de antigüedad, pero con quince (15) bienes, como se puede observar en la figura N°2 del Anexo N°5.

Otro aspecto observado se refiere a los antecedentes académicos registrados de los funcionarios. En el modelo de la base de datos subyacente del sistema, éstos tienen incluso una tabla asignada llamada RH_PE_ANTECEDENTE_ACADEM. Sin embargo, ésta sólo tiene dos registros, en los cuales se encontraron inconsistencias. Por ejemplo, el empleado de RUT10.988.067-1 tiene registrado que su nivel de estudios es "Técnico de nivel superior", sin embargo, su título es "Ingeniero Civil en Computación", que es de carácter universitario (ver figura N° 3 del Anexo N° 5). A su vez, se agregaron algunos registros y el sistema permitió que a una persona que previamente se le asignó un nivel educacional bajo (media incompleta), tuviera como título obtenido una maestría en filosofía, con lo cual se observa inconsistencia en los antecedentes del funcionario.

En virtud de lo anterior, corresponde puntualizar que dicho sistema, no valida ni correlaciona los distintos campos de los antecedentes curriculares, ni el título profesional, ni de la profesión que muestra e ingresa en distintas pestañas. Esto, aparte de ser lógicamente inconsistente, puede causar confusión y no permitiría al sistema validar ciertas opciones durante el cálculo de remuneraciones, como por ejemplo, escalafón y/o asignación de título.

A su vez, se revisaron las horas extras registradas en el sistema, de las cuales, sólo un empleado superó el límite legal de horas diurnas (40 hrs), por una hora (ver detalle en figura N° 4 del Anexo N° 5).

3. Cálculo de nómina

Para verificar que si el sistema calcula debidamente la nómina de horas extraordinarias, se procedió a obtener un listado

⁷ Ver el archivo "Listado funcionarios Presi con Grado extraído de SQL Server por consulta hecha por RCA.xls" o "Listado funcionarios Presi 10 2010" del CD DE ANTECEDENTES.

⁸ Ver el archivo "Listado Liquidaciones Presidencia septiembre 2010.xls" del CD DE ANTECEDENTES.

⁹ Ver el archivo "Listado empleados con grado dinámico 001.xls" del CD DE ANTECEDENTES.



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

completo de éstas, para el mes de septiembre de 2010. Realizada la evaluación de dicha lista, se pudo observar que el cálculo está correcto.

Adicionalmente, se realizó una consulta a todos los registros de la base de datos, buscando remuneraciones o pagos a personas (identificadas por el RUT) que no estuvieran debidamente registradas, no determinándose irregularidades.

4. Licencias

En el módulo de licencia se buscaron licencias que no tuvieran un RUT registrado y no se encontraron anomalías. Los datos de los médicos son debidamente registrados.

El Servicio indica en su respuesta, que durante el año 2010 y primer trimestre del 2011, se ha trabajado en implementar mejoras funcionales al Sistema SIGA. Además, manifiesta que se encuentra en proceso de protocolización de diversos acuerdos de cooperación con el Ministerio de Economía, MINECOM, y el Ministerio Secretaría General de Gobierno, SEGEOB, de forma de dar solución a las observaciones dentro del año en curso.

En mérito de lo anterior, las observaciones se mantienen, por el momento, hasta que este Organismo Contralor realice las verificaciones correspondientes y compruebe la efectividad de las medidas enunciadas.

V. Sistema de Subvenciones Presidenciales

A modo ilustrativo, cabe precisar que en el Informe Final N° 96-1, de 2010, sobre auditoría a las Subvenciones Presidenciales de esta Contraloría General, se indicó que "El presupuesto actualizado de subvenciones, al 31 de marzo de 2010, alcanzó a M\$ 4.943.710, monto que incluye el incremento de M\$ 2.350.000 aprobado mediante decreto N° 191, de 12 de febrero de 2010, del Ministerio de Hacienda, a través del cual se aumentó el presupuesto inicial de M\$2.593.710, aprobado por la ley N° 20.407, de Presupuestos del Sector Público para el año 2010."

El Sistema de Subvenciones Presidenciales está implementado en la intranet del Servicio, desarrollado internamente por el DI en ASP/VBScript y una base de datos administrada con SQL Server. Esta última tiene 24 tablas.

La funcionalidad del sistema (ver detalle en figura N°1 del Anexo N° 6), consiste en llevar un registro de las acciones de cada solicitud de subvención, es decir, se anota cada solicitud que debe ser realizada por un solicitante previamente registrado (ver figura N°2 del Anexo N° 6). Esta petición debe ir acompañada con los documentos respectivos que son almacenados generalmente en formato pdf. El equipo a cargo, verifica la documentación entregada y emite una opinión respecto de la solicitud. El flujo de trabajo sigue con el registro de la decisión de aprobar o no la subvención, y de ser aceptado registrar el monto.

Al ingresar nuevos solicitantes, se constató que es posible ingresar RUT inválidos, direcciones de correo electrónicos



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

completamente numéricos, números de teléfonos compuestos sólo de letras, tal como se puede ver en la figura N°3 del Anexo N° 6. Asimismo, se observó que el campo "cargo" no está restringido en ninguna forma, permitiendo la falta de integridad de información. Al realizar la validación de los datos existentes en la tabla "Solicitantes", se determinaron las anomalías que a continuación se indican:

- Hay 2.553 registros con una llave automática de autoincremento. El número más grande de éste es el 2.557. La diferencia entre el número de registro y llave de autoincremento, deja abierta la posibilidad de eliminar registros sin dejar constancia de ello, y además, generar inconsistencia.
- Existen 2.292 registros con el campo RUT vacío. Asimismo, 214 registros con RUT 0-0, para distintos solicitantes¹⁰.
- Dos registros contienen el mismo RUT: 71.836.200-8, los cuales difieren sólo en dos campos: fono y mail. Lo anterior, muestra una gran debilidad en el sistema al momento de controlar la inconsistencia y restringir la posibilidades de fraude.

Lo precedentemente expuesto, indica que hay inconsistencia en la base de datos y falta de validación estructural y lógica en la misma.

En cuanto al registro de solicitudes, en éste se debe ingresar el responsable de procesar la solicitud (evaluador), sin embargo, se verificó que se pueden ingresar datos libremente, lo que permite responsabilizar a cualquiera, o a nadie, ya que el campo no es obligatorio (Ver figura N°4 del Anexo N°6).

Al analizar la tabla "Seguimiento", se constató que sólo tiene dos registros. También que muchas solicitudes no están con todos los antecedentes necesarios, a pesar del tiempo que llevan registradas.

Debido a la falta de consistencia y lo incompleto de los datos existentes, se consultó al Departamento de Informática de la Presidencia, el que manifestó que el sistema es usado sólo como un apoyo de registro paralelo por sus usuarios y que éstos llevan un registro en excel y procesan las solicitudes en forma manual.

En mérito de los antecedentes antes enunciados, es posible indicar que el sistema no es usado adecuadamente, y no opera como soporte y validación en el procesamiento de las solicitudes, por lo tanto, la información ahí almacenada no es representativa, ni confiable. Además, el uso de planillas excel, tal como lo señaló el DI, no subsana las falencias y riesgos señalados anteriormente, es más, existe un conjunto de riesgos adicionales por la utilización de las mencionadas planillas.

En la respuesta del Servicio se manifiesta que durante el primer semestre de 2011 se implementará un nuevo sistema que responda a nuevos procedimientos y controles administrativos, que han sido

¹⁰ Ver hoja "tabla de solicitantes" del archivo "Datos de la base de subvenciones.xls" del CD DE ANTECEDENTES.



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

diseñados durante el año 2010. Por lo tanto, se mantiene la observación hasta que no se valide la efectiva implementación de dicho sistema.

VI. CONCLUSIONES

Del resultado de la auditoría practicada, así como del análisis y ponderación de los antecedentes aportados en la respuesta a las observaciones formuladas por esta Contraloría General, cabe concluir que la Presidencia de la República ha iniciado acciones que han permitido solucionar, en parte, las observaciones formuladas, cuya efectividad será evaluada en una próxima visita de auditoría.

No obstante lo anterior, corresponde que el Servicio adopte, a lo menos, las siguientes medidas a fin de subsanar las debilidades que aún se mantienen:

1. En cuanto al acápite III, punto 1, designar un ministro de fe, acorde a lo dispuesto en el decreto supremo N° 77, de 2004, del Ministerio Secretaría General de la Presidencia.

2. Formalizar el procedimiento de respaldo mensual de las comunicaciones electrónicas, cuyo proceso sea avalado por el ministro de fe mencionado en el punto anterior.

3. Respecto al acápite III, punto 2, terminar los proyectos de interoperabilidad del sistema de Correspondencia de la Ciudadanía con el Presidente, cuidando que éstos den cabal cumplimiento a lo consignado en el decreto supremo N° 81, de 2004, del Ministerio citado.

4. En referencia al acápite III, punto 3, definir con claridad la metodología de difusión de la política de seguridad.

5. Implementar una política formal de clasificación y etiquetado de los documentos electrónicos y sistemas informáticos.

6. Establecer formalmente una política de seguridad física.

7. Crear un sitio externo de respaldo y definir la política de acceso físico y lógico a dicho sitio.

8. Incluir en el "Procedimiento de formateo de discos duros" definiciones administrativas y prácticas faltantes. Por ello corresponde determinar quién realiza el proceso, cómo se certifica, cómo se asegura que toda máquina que se dé de baja pase por éste, identificando al responsable, entre otros elementos.

9. Establecer una metodología o política oficial, que establezca instrucciones para el personal sobre el manejo adecuado de los identificadores y de las claves de acceso, como el largo, formato, cambio periódico, entre otros.

10. Promover las buenas prácticas para reducir el riesgo de acceso no autorizado, como por ejemplo, la pantalla limpia.



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

11. Establecer un proceso formal de autorización de acceso a las redes y sus servicios.

12. Formalizar un plan de contingencia que asegure la continuidad de las operaciones críticas.

13. Tener un cronograma de revisiones periódicas que indique explícitamente que se evaluará la efectividad de la política, el costo e impacto de los controles en la eficiencia del negocio y los cambios de tecnología. La política de seguridad deberá incluir procedimientos de delegación de autoridad para ejecutar acciones de emergencia en los sistemas y los procedimientos correspondientes.

14. Definir formalmente procedimientos para el etiquetado y la manipulación de los documentos electrónicos.

15. Evaluar la posibilidad de tener seguros para los equipos fuera de la organización. Establecer formalmente la obligación de firmar el documento de no divulgación para todas las visitas a las instalaciones sensibles y de procesamiento.

16. Establecer un procedimiento formal para certificación y mantención de los sistemas.

17. Formalizar un plan de contingencia.

18. Respecto al acápite III, punto 4, formalizar y difundir una guía oficial de protección de las casillas electrónicas, acorde a lo establecido en el decreto supremo N° 93, de 2006, del MINSEGPRES.

19. En cuanto al acápite III, punto 5, poner en marcha las recomendaciones de la guía de accesibilidad para discapacitados en el sitio web.

20. En relación con el acápite IV, sobre el sistema SIGA Personal-Remuneraciones, el Servicio deberá mejorar la validación de bienios. Por otro lado, en caso de conservar los registros que contienen la información de los antecedentes académicos del personal, debe arbitrar las medidas para mejorar la validación, el registro y consistencia de éstos. Asimismo, controlar las horas extras diurnas, en caso que se supere el máximo legal.

21. Respecto al acápite V, sobre el Sistema de Subvenciones Presidenciales, en caso de no ser reemplazado, la Presidencia de la República deberá tomar las acciones correctivas respecto a lo observado por esta Entidad de Control.

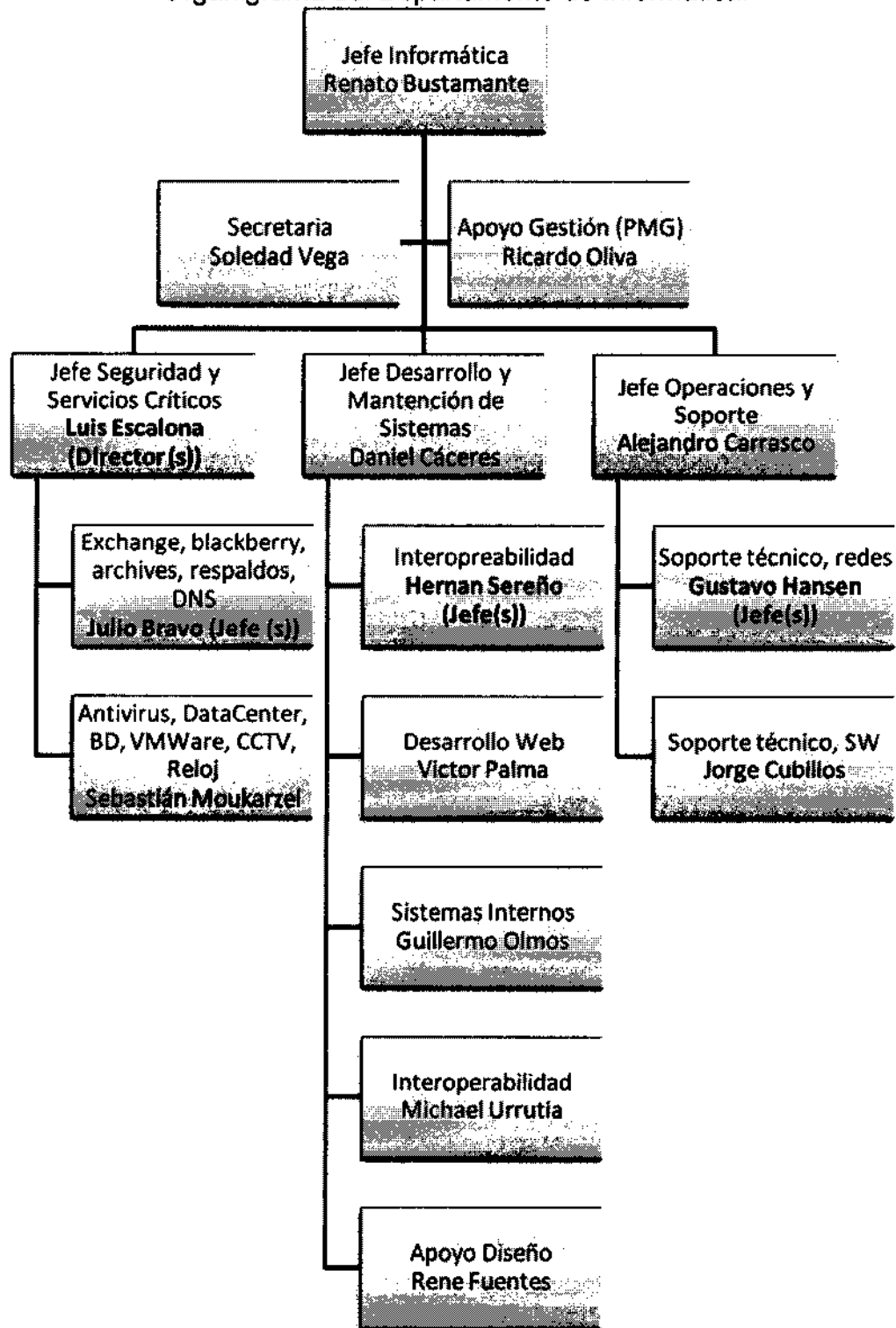
Saluda atentamente a Ud.

MARÍA CRISTINA CALDERÓN VIDAL
JEFE
ÁREA ADMINISTRACIÓN GENERAL
Y DEFENSA NACIONAL



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

ANEXO N° 1
Organigrama del Departamento de Informática.



9/8



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

ANEXO N° 2
Equipos Data Center

[REDACTED]						
1	Corning	-	-	-	-	Organizador de FFOO Entel
2	Corning	-	-	-	-	Organizador de FFOO Entel
3	Lucent	-	-	-	-	Patch FFOO
4	Lucent	-	-	-	-	Patch FFOO
5		-	-	-	-	Patch FFOO
6	ICC	-	-	-	-	Patch de FFOO Telmex
7	Trimex	-	-	-	-	Organizador de FFOO
8		-	-	-	-	Organizador de FFOO GTD
9	Ruby	-	9	-	-	Transceiver Entel - Presidencia
9	Ruby	-	9	-	-	Transceiver Entel - Carabineros
9	Ruby	-	-	-	-	Transceiver Desconectado
9	Ruby	-	-	-	-	Transceiver Desconectado
9	IMC	-	9	-	-	Transceiver GTD - Holanda
10	APC	EMS AP9320	10	-	-	SN: ZA0623020516
10	Paradox	VD710	-	-	-	Discador del Monitor de Ambiente DC
11	Trimer	-	-	-	-	Patch RJ45
12		-	-	-	-	Organizador de Cables
13	Trimer	-	-	-	-	Patch RJ45
14		-	-	-	-	Organizador de Cables
15	Trimer	-	-	-	-	Patch RJ45
15B	Cisco	WLC 2106	10	-	-	SN: JMX1214K02T
15B	Castelle	Fax Press 2500	10	-	-	SN: 8340565
16B	Fortinet	Fortianalyzer 100A	10	-	-	SN: FL100A2106000681
16		-	-	-	-	Organizador de Cables
17	Cisco	WS6509	1 y 2	-	-	SN: SMG1244N8ZL
18	Siemon	-	-	-	-	Patch RJ45
19	Cisco	RPS2300	3	-	-	SN: FD013035GKH
20	Cisco	Cisco 3560	10	-	-	SN: FOC1249W054
21	Cisco	Cisco 2621	10	-	-	SN: FHK1103F122
22	Systimax	-	-	-	-	Patch RJ45
23	Krone	-	-	-	-	Patch RJ11



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

Ítem	Marca	Modelo	Cantidad	Características	Valor	Observaciones
41	Fortigate	FG-800	9	-	-	SN: FGT8002605500321
40	Fortigate	c	3	-	-	SN: FGT8002605500317
35 -37	DELL EMC	CX3-10 Enclosure 1	-	-	-	ST: FZC5RD1
34	DELL EMC	Fuentes de poder	4 y 3	-	-	-
33	DELL EMC	SPA Y SPB	-	-	-	ST: HZC5RD1
40B	DELL	Power Connect 2724	9	-	-	ST: 159JSB1
39 B	Brocade	200F	4	-	-	ST: 15K55C1
38 B	Brocade	200F	9	-	-	ST: FRJ55C1
31 - 32	DELL	Power Edge 2950	9 y 4	2 x Xeon E5410 2,33Ghz (8 cores)	4 GB	ST: 9Y5PJF1
29 - 30	DELL	Power Edge 2950	9 y 4	2 x Xeon E5410 2,33Ghz (8 cores)	32 GB	ST: 295PJF1
27 - 28	DELL	Power Edge 2950	9 y 4	2 x Xeon E5410 2,33Ghz (8 cores)	32 GB	ST: 695PJF1
25 - 26	DELL	Power Edge 2950	3 y 4	2 x Xeon E5410 2,33Ghz (8 cores)	32 GB	ST: 595PJF1
24	DELL	Power Edge Rack Console 15FP	4	-	-	SN: 3HV2
21 - 22	DELL	TL2000	3	-	-	ST: 9128XD1
19 - 20	Dell	PowerEdge 2950	4 y 3	2 x 5130 2Ghz (4 cores)	4 GB	ST: 4WZZYC1
18	PineApp	Archive Secure	3	-	-	
17	PineApp	Enclosure	3	-	-	Enclosure 4 discos (PineApp)

[Handwritten mark]



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

Ubicación (Número)	Marca	Modelo	Cantidad	Procesador	Memoria	ST
15	ContentKeeper	CK-1046-LE2	3	-	-	
13 - 14	DELL	TL2000	6	-	-	ST: 98NRJL1
11 - 12	DELL	TL2000	6	-	-	ST: 78NRJL1
9	DELL	PowerEdge 1950	4 Y 9	2 x Xeon E5405 2Ghz (4 cores)	2 GB	ST: CHDL6G1
10	Thales	Web Sentry	9	-	-	
10	Thales	Lector Tarjeta Seguridad	9	-	-	
4 - 7	SunShine	Armado	10	Quad Q8200 2,3Ghz (4 cores)	2 GB	SN: 62590542
1 - 3	Caja Transformadres CCTV		10	-	-	
PISO-Atrás	DELL	PE830	5	P4 3,6Ghz (2 cores)	2 GB	ST: HYTJ1B1
28 - 38 B	DELL	CMN1012	4	-	-	ST: 436QRC1

Ubicación (Número)	Marca	Modelo	Cantidad	Procesador	Memoria	ST
39 - 41	DELL	Enclosure 2 CX3-10	6 y 5	-	-	ST: JDP0HH1
37 - 38	Storeva ult	S500	8 Y 6	-	-	SN: QMNCSN8 040065
36	Cisco	ASA 5510	5	-	-	SN: JMX1247
35	Cisco	CD MARS 55	6	-	-	SN: AZHH8270 04
33	Dell	PowerEdge 1950	Apagado	Xeon Woodcrest 5110	512 MB	ST: 1FPSBC1
32	Dell	PowerEdge 1950	6	Xeon Woodcrest 5110	512 MB	ST: HDPSBC1
30 - 31	DELL	PowerEdge 2950	5 y 8	2 x E5335 2Ghz (8 cores)	2 GB	ST: 8P40WD1
28 - 29	DELL	PowerEdge 2950	8 y 6	2 x 5130 2Ghz (4 cores)	4 GB	ST: 8WZZYC1

Handwritten mark



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

26 - 27	DELL	PowerEdge 2950	6 y 8	2 x 5130 2Ghz (4 cores)	8 GB	ST: 6WZZYC1
24	DELL	Power Edge Rack Console 15FP	5	-	-	SN: 345F
22	DELL	Power Edge	8 y 5	Intel Pentium III 1.26GHz	1 GB	ST: 4CLKS11
20 - 21	NEC	Express 5800 120Rd	5 y 6	Intel Pentium III 1.13 Ghz	1 GB	SN: 303518700 1
17 - 18	DELL	Power Edge R710	8 y 6	2 x E5530 2,4Ghz (16 cores)	6 GB	ST: 2TZSSL1
11 - 12	DELL	Power Edge R710	5 y 8	2 x E5560 2,8Ghz (16 cores)	12 GB	ST: 52WWGM 1
9 - 10	DELL	Power Edge R710	5 y 5	2 x E5560 2,8Ghz (16 cores)	12 GB	ST: 42WWGM 1
7 - 8	DELL	Power Edge R710	7 y 8	2 x E5560 2,8Ghz (16 cores)	12 GB	ST: 32WWGM 1
ARRIBA-ATRÁS	DELL	SW-KVM	-	-	-	SN: AB98
Interior	Dell	KVM	-	-	-	ST: FGWRV91

26 - 27	DELL	Power Edge R710	7 y 11	2 x E5520 2,27Ghz (8 cores)	4 GB	ST: CSX5VL1
24	DELL	CONSOLA	7	-	-	SN: AG40
32 - 33	DELL	Power Edge R710	7 y 11	2 x E5560 2,8Ghz (16 cores)	6 GB	ST: BPG7JL1
34 - 35	DELL	Power Edge R710	7 y 11	2 x E5560 2,8Ghz (16 cores)	6 GB	ST: DPG7JL1
14 - 15	DELL	PowerEdge 2950	7	Xeon Clovertown E5310	8 GB	ST: HVKVHF1
28 - 37 INT	DELL	KVM	7	-	-	ST: 1NDL9F1
28 - 29	DELL	Power Edge R710	7 y 11	2 x E5530 2,4Ghz (16 cores)	6 GB	ST: JSZS5L1
30 - 31	DELL	Power Edge R710	7 y 11	2 x E5530 2,4Ghz (16 cores)	6 GB	ST: 1VZS5L1
16 - 17	DELL	Power Vault NX3100	7 y 11	Quad Core Intel Xeon E5506, 2.13GHz	6 GB	ST: 9SCSVN1

48



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

Ubicación						
ARRIBA-ATRÁS	DELL	SW-KVM	-			SN: ABC6



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

ANEXO N° 3
Servidores Virtuales

CP	Procesador	OS	Memoria	Descripción
1	Intel Xeon E5410 2,33Ghz	Microsoft Windows 2000 Server	1024 MB	SERVIDOR WEB APP GPS MOVILIZACIÓN
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	DOMINIO Y CORREO PARA LA COPUCHA
1	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	APLICACIÓN DE PLANIFICACION Y CONTROS - PSICUS
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	3072 MB	SERVIDOR BLACKBERRY PRESIDENCIA
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	SERVIDOR BASES DE DATO DESARROLLO
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	2048 MB	SERVIDOR BLACKBERRY IMAGEN DE CHILE
1	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	CONTROL DE ACCESO (RELOJES)
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	APLICACIÓN DEXON
1	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	2048 MB	SERVIDOR BASES DE DATO TESTING
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	4096 MB	SERVIDOR WEB - SITIOS
4	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (64-bit)	4096 MB	BASES DE DATO SIGP
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	3072 MB	SERVIDOR WEB - SITIOS
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	CONTROLADOR DE DOMINIO PRESIDENCIA Y DNS PRIMARIO
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Enterprise Edition (64-bit)	2048 MB	DOMINIO Y CORREO PARA IMAGEN DE CHILE
4	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Enterprise Edition (64-bit)	4096 MB	HUB TRANSPORT - OWA - CORREO PRESIDENCIA

✍



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

GPU Cpu				
4	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (64-bit)	4096 MB	HUB TRANSPORT - OWA - CORREO PRESIDENCIA
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	4096 MB	DOMINIO Y CORREO PARA COMISION BICENTENARIO
1	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	2048 MB	SERVIDOR WEB TRANSPARENCIA
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	3072 MB	BASE DE DATOS DEXON
1	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	SERVIDOR FTP
1	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	SERVIDOR DE SEGURIDAD
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	2048 MB	SERVIDOR WEB - SITIOS
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	RECEPTOR APLICACIÓN GPS MOVILIZACION
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	4096 MB	DOMINIO Y CORREO PARA COMISION VALECH
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	2048 MB	GATEWAY DE CORREO BICENTENARIO
1	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	3072 MB	CONTROLADOR DE DOMINIO PRESIDENCIA, DNS SECUNDARIO Y CONSOLA ANTIVIRUS
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	CONTROLADOR DE DOMINIO PRESIDENCIA
1	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	SHAREPOINT INFORMÁTICA
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	BASE DE DATOS MOVILIZACIÓN Y CONTROL ASISTENCIA
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	WEB INTRANET PRESIDENCIA



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

Cantidad	Procesador	Sistema Operativo	Memoria RAM	Función
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	GATEWAY DE CORREO PRESIDENCIA
4	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	2048 MB	CONTROLADOR DE DOMINIO PRESIDENCIA
1	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	2048 MB	SERVIDOR WEB TESTING - SITIOS
1	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Enterprise Edition (32-bit)	2040 MB	SERVIDOR WEB DESAROLLO - SITIOS
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	DNS EXTERNO PRESIDENCIA
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Enterprise Edition (64-bit)	4096 MB	SERVIDOR BLACKBERRY PRESIDENCIA
1	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	CONTROL DE HUELLA CASINO PRESIDENCIA
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Enterprise Edition (64-bit)	4096 MB	BASE DE DATOS CORREO PRESIDENCIA
4	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Web Edition	4096 MB	SERVIDOR WEB – SITIOS
1	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Enterprise Edition (64-bit)	2048 MB	BASE DE DATOS CORREO PRESIDENCIA
1	Intel Xeon E5410 2,33Ghz	Suse Linux (64-bit)	512 MB	SERVIDOR DE MONITOREO SERVIDORES Y SERVICIOS
1	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	SERVIDOR DE ARCHIVOS COMPARTIDOS
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows XP Professional (32-bit)	2048 MB	CONTROL DE ACCESO CASINO PRESIDENCIA
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	GATEWAY DE CORREO
1	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (64-bit)	2048 MB	SERVIDOR DE PRUEBAS VARIAS
1	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	1024 MB	SERVIDOR DE ACTUALIZACIONES PRODUCTOS MICROSOFT

24



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

1	Intel Xeon E5410 2,33Ghz	Microsoft Windows XP Professional (32-bit)	512 MB	WINDOWS XP PARA PRUEBAS VARIAS
1	Intel Xeon E5410 2,33Ghz	Microsoft Windows XP Professional (32-bit)	512 MB	PARA EL REDIMENSIONAMIENTO DE DISCOS VIRTUALES
4	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Standard Edition (32-bit)	4076 MB	SERVIDOR BASES DE DATO SITIOS WEB
2	Intel Xeon E5410 2,33Ghz	Microsoft Windows Server 2003, Enterprise Edition (32-bit)	3072 MB	SERVIDOR BASES DE DATO APLICACIONES ADMINISTRATIVAS

48



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

ANEXO N° 4

Listado de sistemas bajo administración del Departamento de Informática

Prensa	www.fotopresidencia.cl	ASP	Terminado	Evolutivo	
Prensa	Archivo Fotográfico Presidente	ASP	Desarrollo		
Prensa	www.prensapresidencia.cl	ASP	Terminado	Evolutivo	
Gabinete Primera Dama	www.fundaciones.cl	ASP	Desarrollo		Actualmente en proceso de Rediseño
Comisión Derechos Humanos	www.comisionvalech.gov.cl	HTML	Terminado	Evolutivo	
Comisión Bicentenario	www.chilebicentenario.cl	ASP.NET Framework 3.5	Terminado	Evolutivo	
Segegob	www.redprotege.gov.cl	ASP.NET Framework 2.0	Terminado	Evolutivo	
Fundación Imagen País	www.fundacionimagendechile.cl	ASP.NET Framework 3.5	Terminado	Evolutivo	
Fundación Imagen País	www.hablamedechile.cl	ASP.NET Framework 2.0	Terminado	Evolutivo	
Fundación Imagen País	www.thisischile.cl	ASP.NET Framework 3.5	Terminado	Evolutivo	
Dirección Administrativa	intranet.presidencia.cl	ASP.NET Framework 2.0	Terminado	Evolutivo	
Gabinete Presidencial	Sistema Seguimiento Institucional de Correspondencia Presidencial (Interoperabilidad)	ASP.NET Framework 1.1	Terminado	Evolutivo	
Dirección Administrativa	www.presidencia.cl/transparencia	HTML	Terminado	Evolutivo	
Unidad Web	www.gobiernodechile.cl	Php / HTML		Evolutivo	CMS de desarrollo en Wordpress con migración a html para producción

ADMINISTRATIVA	SIGP-MIA Movilización	Delphi 7	Terminado	Evolutivo	
ADMINISTRATIVA	SIGP-MIA Obras de Arte	Delphi 7	Terminado	Evolutivo	
ADMINISTRATIVA	Sistema Central Telefónica	Visual Basic 6.0	Terminado	Evolutivo	
GABINETE	Subvenciones Presidenciales	ASP – VBScript	Terminado	Evolutivo	
ADMINISTRATIVA	Sistema de Control de Gastos	Visual Basic 2003	Terminado	Evolutivo	
GABINETE	PNUD	Delphi 7	Terminado	Correctivo	
ADMINISTRATIVA	Sistema Control de Acceso Visitas (CAV) Pauta	Visual Basic 6.0	Terminado	Correctivo	
DINFO	HOTH	Sharepoint	Terminado	Correctivo	



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

		2003			
Origen	Sistema / Proyecto	Código fuente	Estado	Mantenimiento	
*GABINETE	Servicio Web Seguimiento Institucional (Interoperabilidad 2010)	ASP.NET	Terminado	Evolutivo	Próximo Web Service XML
ADMINISTRATIVA	Intranet.presidencia.cl		Terminado	Evolutivo	
DDHH	www.comisionvatech.gov.cl	HTML	Terminado	Evolutivo	
PRENSA	www.fotopresidencia.cl	ASP 1.0	Terminado	Evolutivo	
PRENSA	Archivo Fotográfico Presidente	ASP 1.0	Terminado	Evolutivo	
DIR. ADM	Intranet/Evaluación Desempeño	ASP 1.0	Terminado	Evolutivo	
Origen	Sistema / Proyecto	Código fuente	Estado	Mantenimiento	
ADMINISTRATIVA	SIGA-Existencias-Abastecimiento	.NET Framework 3.5	Desarrollo		
ADMINISTRATIVA	Mantención Técnica DEXON	Dexon	Evaluación		
ADMINISTRATIVA	Control de asistencia – ASISCAD	.NET Framework 2.0	Terminado	Evolutivo	Desarrollo externo
ADMINISTRATIVA	Control de asistencia - FINGERACCES	.NET Framework 2.0	Terminado	Evolutivo	Desarrollo externo
ADMINISTRATIVA	Intranet/Control Asistencia	.NET Framework 2.0	Terminado	Correctivo	
ADMINISTRATIVA	SIGA-Personal-Remuneraciones	.NET Framework 1.1	Terminado	Evolutivo	
ADMINISTRATIVA	Sistema Bienestar	.NET Framework 1.1	Terminado	Correctivo	
ADMINISTRATIVA	Activo Fijo DEXON	Dexon	Planificación		El usuario se encuentra depurando la información
ADMINISTRATIVA	Minutas Casino		Desarrollo		Urgente

28



CONTRALORÍA GENERAL DE LA REPÚBLICA

DIVISIÓN DE AUDITORÍA ADMINISTRATIVA

ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

Sistema Integrado de Gestión Administrativa (SIGA) Versión: 1.0. 2006. 23/03 [Antecedentes Académicos]

Personal > Remuneraciones > Registrar Tablas Muestras > Control Asistencia > Verificar Ayuda

Empleado

RUT: 10988867

Nombre: QUIRONES MOLINA, JORGE ALFONSO

Nivel de Estudios	Año Inicio	Año Término	Institución	Título Obtenido	Período Estudio	Fide	Paralelo
TECNICO NIVEL SUPERIOR COMPLETA							

Usuario: PROHLEVAuditor Servidor: 172.20.1.100 Base de Datos: SIGA/AUDIT Período Vigente: NOVIEMBRE 2010 Antecedentes Académicos

Figura 3: Lo que dice SIGA en Antecedentes académicos.

SQL Server Enterprise Manager [New View in 'SIGA_AUDIT' (172.20.1.100)]

Archivo Verbase Ayuda

Query Editor - SQL Server Enterprise Manager

```

SELECT TOP 100 PERCENT dbo.RH_PER_EMPLEADO.RUT, dbo.RH_PER_EMPLEADO.DV, dbo.RH_PER_EMPLEADO.APELLIDO_PATERNO,
dbo.RH_PER_EMPLEADO.APELLIDO_MATERNO, dbo.RH_PER_EMPLEADO.NOMBRES, dbo.RH_REM_LIQUIDACION.NUMERO_HORAS_EXTRAS,
dbo.RH_REM_PERIODO.HORAS_EXTRAS_LEGAL_DIURNAS, dbo.RH_REM_PERIODO.DESCRIPCION_PERIODO,
dbo.RH_REM_PERIODO.HORAS_EXTRAS_LEGAL_NOCTURNAS, dbo.RH_REM_ITEM.DESCRIPCION_CORTA,
dbo.RH_REM_LIQUIDACION.ITEM_ID
FROM dbo.RH_REM_PERIODO INNER JOIN
dbo.RH_REM_LIQUIDACION ON dbo.RH_REM_PERIODO.PERIODO_ID = dbo.RH_REM_LIQUIDACION.PERIODO_ID AND
dbo.RH_REM_PERIODO.HORAS_EXTRAS_LEGAL_DIURNAS < dbo.RH_REM_LIQUIDACION.NUMERO_HORAS_EXTRAS INNER JOIN
dbo.RH_PER_EMPLEADO ON dbo.RH_REM_LIQUIDACION.EMPLEADO_ID = dbo.RH_PER_EMPLEADO.EMPLEADO_ID INNER JOIN
dbo.RH_REM_ITEM ON dbo.RH_REM_LIQUIDACION.ITEM_ID = dbo.RH_REM_ITEM.ITEM_ID
WHERE (dbo.RH_REM_LIQUIDACION.ITEM_ID = 15)
ORDER BY dbo.RH_PER_EMPLEADO.RUT
  
```

RUT	DV	APELLIDO_PATERNO	APELLIDO_MATERNO	NOMBRES	NUMERO_HORAS_EXTRAS	HORAS_EXTRAS_LEGAL_DIURNAS	DESCRIPCION PERIODO	HORAS_EXTRAS_LEGAL_NOCTURNAS	DESCRIPCION_CORTA	ITEM_ID
5	AAZC	PERZOA	MIGUEL ANGEL		41	40	2010-10	999	HRS.EXT.25%	15

Inicio

Figura 4 Consulta sobre horas extras que sobrepasen el límite legal para el periodo de las horas máximas diurnas.(=15 código para las diurnas)

88



CONTRALORÍA GENERAL DE LA REPÚBLICA

DIVISIÓN DE AUDITORÍA ADMINISTRATIVA

ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

ANEXO N° 6

Captura de pantallas del sistema de subvenciones presidenciales

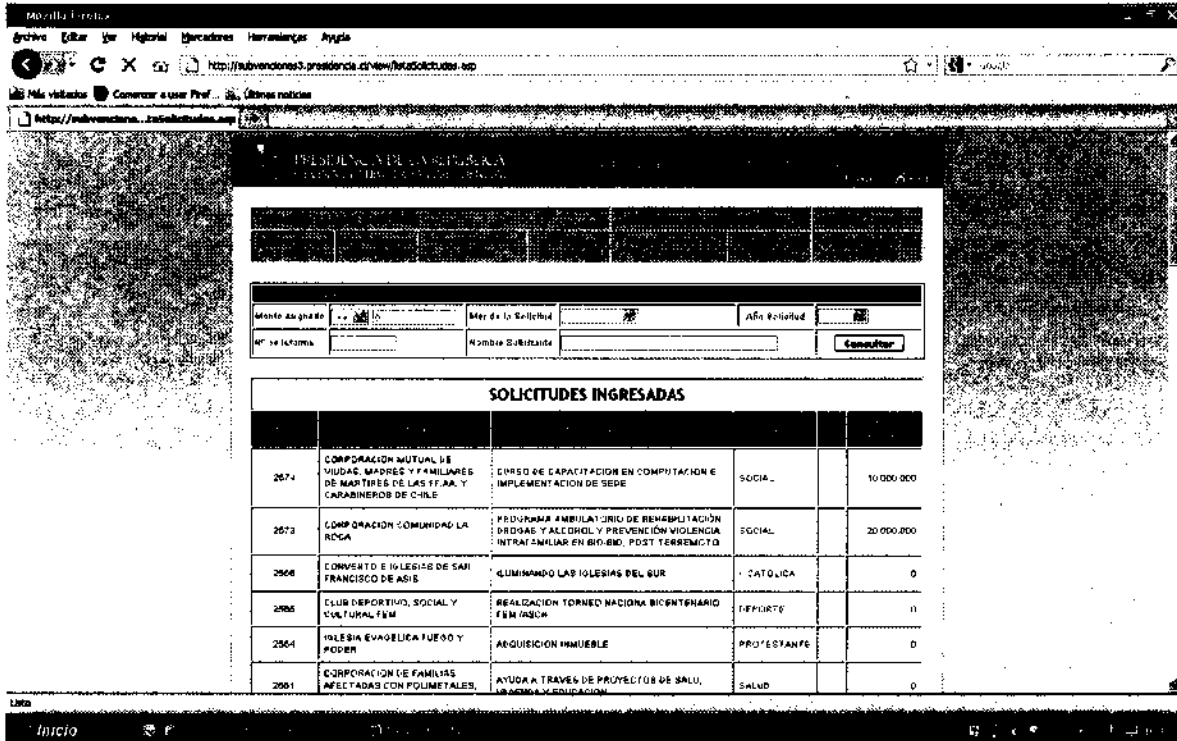


Figura 1: Pantalla Inicial

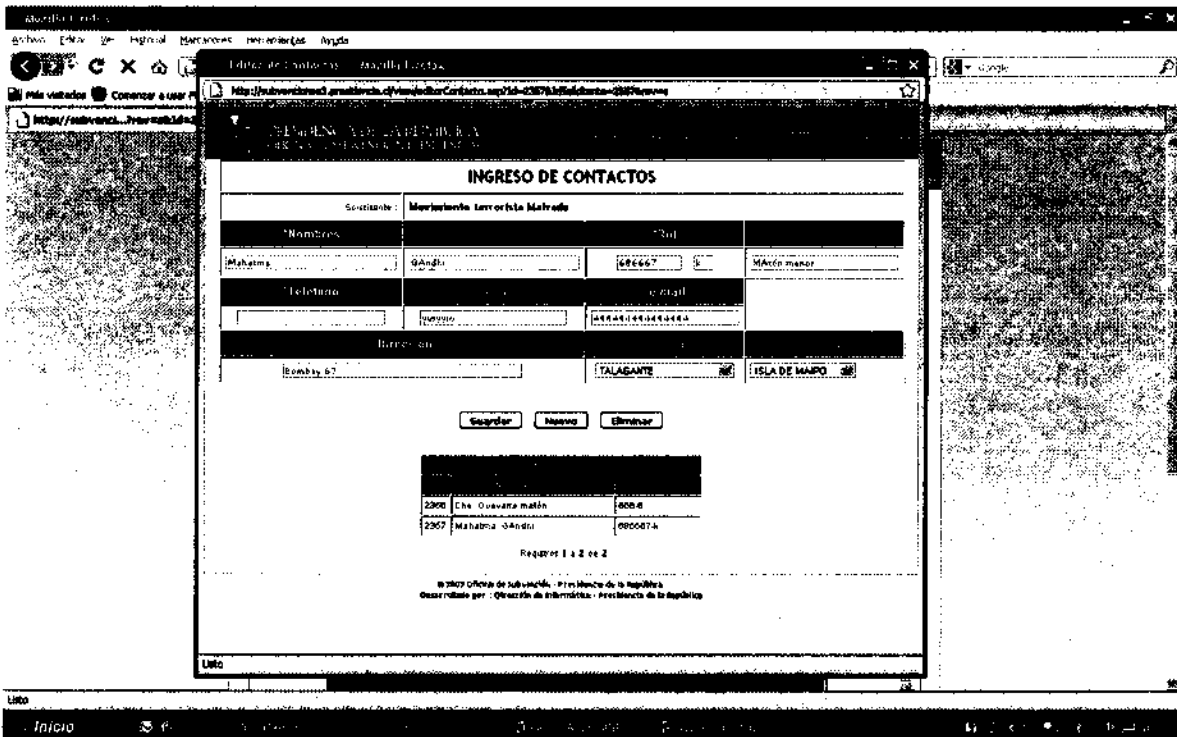


Figura 2: Ingreso de contactos. Notar Fono con solo letras y RUT inventado que no valida.

✗



CONTRALORÍA GENERAL DE LA REPÚBLICA
DIVISIÓN DE AUDITORÍA ADMINISTRATIVA
ÁREA ADMINISTRACIÓN GENERAL Y DEFENSA NACIONAL

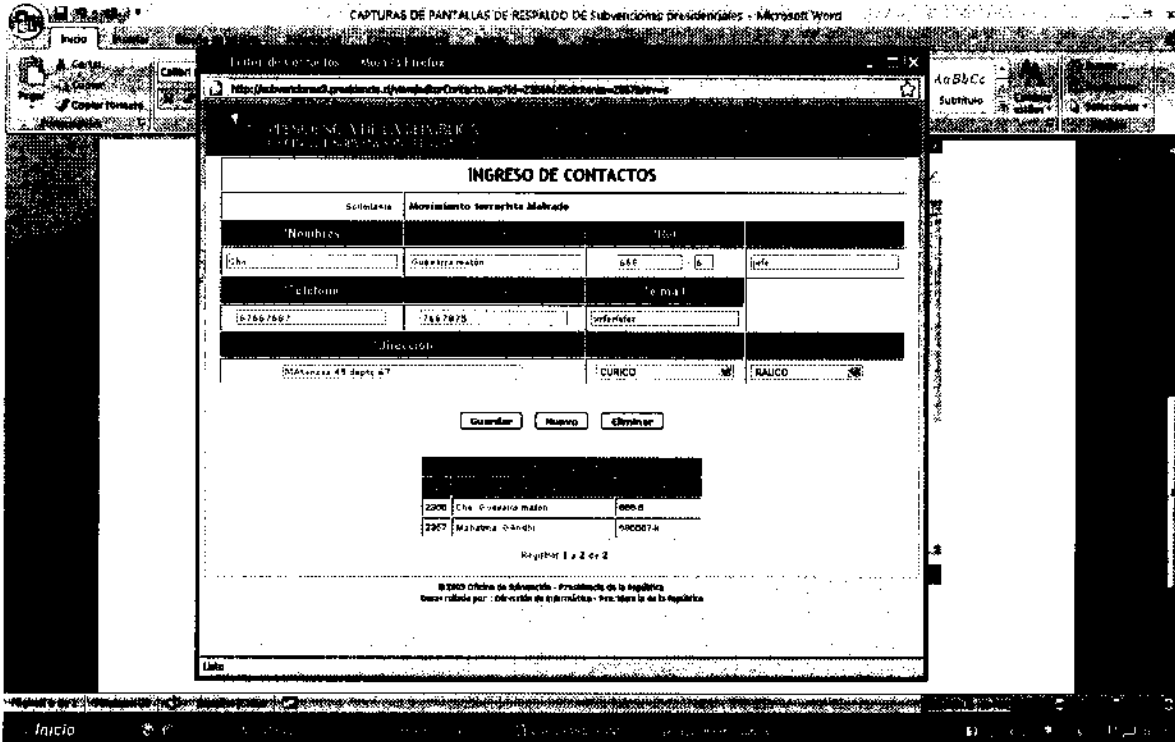


Figura 3: Otro contacto ingresado, RUT inválido.

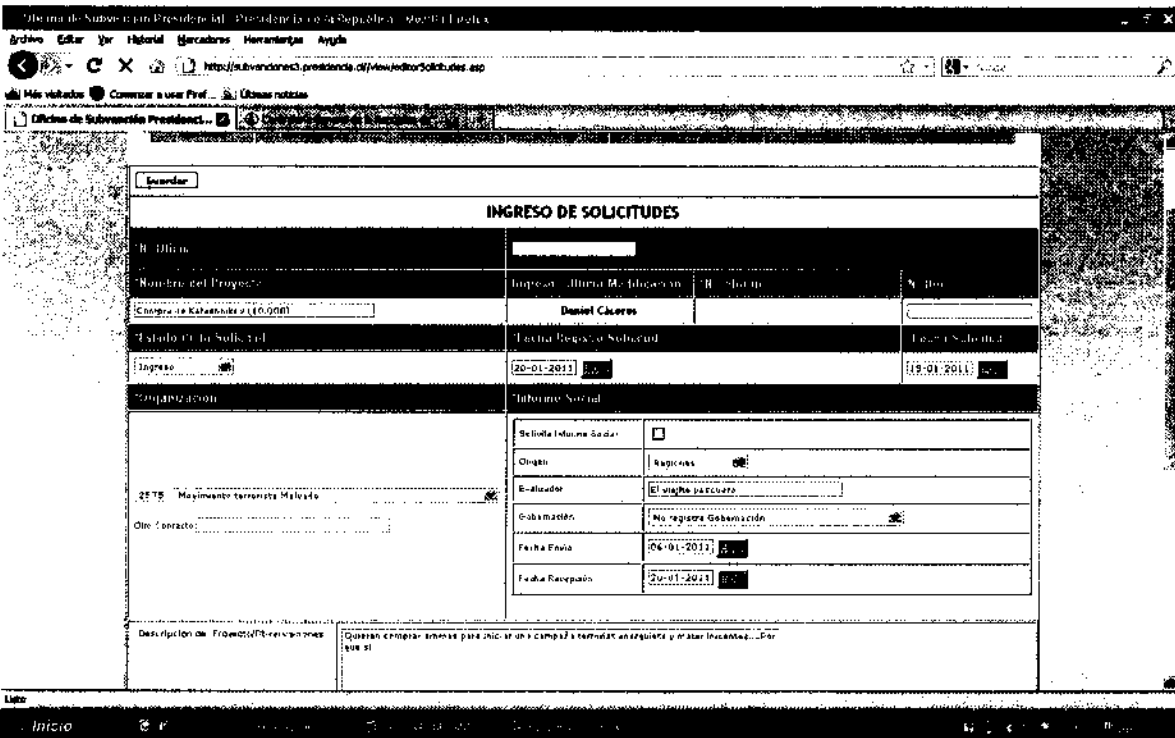


Figura 4: Ingreso de una solicitud. Notar evaluador: "El viejo pascuero".

98



www.contraloria.cl