



INFORME FINAL

MUNICIPALIDAD DE BULNES

INFORME N°92/2019

3 DE ABRIL DE 2019



POR EL CUIDADO Y BUEN USO
DE LOS RECURSOS PÚBLICOS

CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

REF. N° 400.542/2019
UCE. N° 96/2019

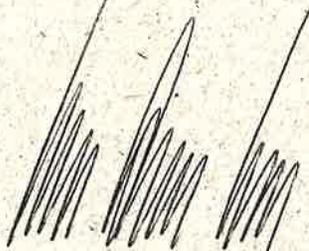
REMITE INFORME FINAL QUE INDICA.

CONTRALORIA GENERAL DE LA REPUBLICA
REGION 16
03 ABR 2019 N° 792
CHILLÁN, 
21620190403792

Adjunto, remito a Ud., para su conocimiento y fines pertinentes, copia del Informe Final N° 92, de 2019, debidamente aprobado, que contiene los resultados de la fiscalización a las tecnologías de información en la Municipalidad de Bulnes.

Sobre el particular, corresponde que esa autoridad adopte las medidas pertinentes, e implemente las acciones que en cada caso se señalan, tendientes a subsanar las situaciones observadas.

Saluda atentamente a Ud.,


Mario Quezada Fonseca
Contralor Regional de Ñuble
Contraloría General de la República


AL SEÑOR
ALCALDE
MUNICIPALIDAD DE BULNES
BULNES





CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

REF. N° 400.542/2019
UCE: N° 97/2019

REMITE INFORME FINAL QUE INDICA.

CONTRALORÍA GENERAL DE LA REPÚBLICA
REGIÓN 16

03 ABR 2019

N° 793

CHILLÁN,

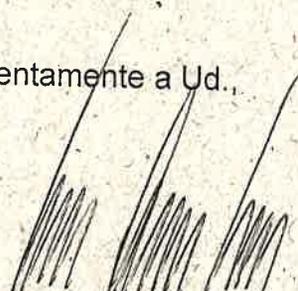


21620190403793

Adjunto, remito a Ud., para su conocimiento y fines pertinentes, copia del Informe Final N° 92, de 2019, debidamente aprobado, que contiene los resultados de la fiscalización a las tecnologías de información en la Municipalidad de Bulnes, con el fin de que, en la primera sesión que celebre el concejo municipal, desde la fecha de su recepción, se sirva ponerlo en conocimiento de ese órgano colegiado entregándoles copia del mismo.

Al respecto, Ud. deberá acreditar ante esta Contraloría Regional, en su calidad de secretario del concejo y ministro de fe, el cumplimiento de este trámite dentro del plazo de diez días de efectuada esa sesión.

Saluda atentamente a Ud.,


Mario Quezada Fonseca
Contralor Regional de Ñuble
Contraloría General de la República




(S) 15/04/2019

 AL SEÑOR
SECRETARIO MUNICIPAL
MUNICIPALIDAD DE BULNES
BULNES



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

REF. N° 400.542/2019
UCE. N° 98/2019

REMITE INFORME FINAL QUE INDICA.

CONTRALORÍA GENERAL DE LA REPÚBLICA
REGIÓN 16

03 ABR 2019

N° 794

CHILLÁN,



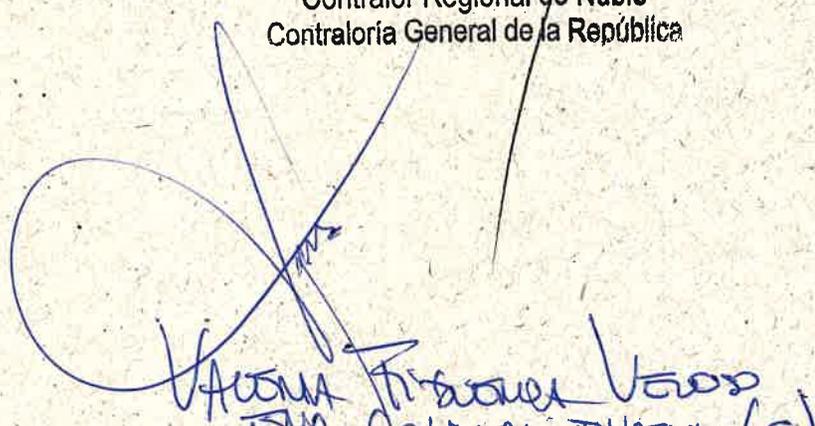
Adjunto, remito a Ud., para su conocimiento y fines pertinentes, copia del Informe Final N° 92, de 2019, debidamente aprobado, que contiene los resultados de la fiscalización a las tecnologías de información en la Municipalidad de Bulnes.

Al respecto, Ud. deberá acreditar en el Sistema de Seguimiento y Apoyo CGR, que esta Entidad de Control puso a disposición de las entidades públicas a contar del 2 de julio de 2018, en conformidad con lo establecido en el oficio N° 14.100, de 2018; de este Órgano Contralor, aquellas observaciones que se mantienen y que fueron categorizadas como MC y LC, descritas en el mismo Anexo N°4 del mencionado informe final.

Saluda atentamente a Ud.,


Mario Quezada Fonseca
Contralor Regional de Ñuble
Contraloría General de la República


AL SEÑOR
DIRECTOR DE CONTROL INTERNO
MUNICIPALIDAD DE BULNES
BULNES


Valeria Frisones Urrutia
CUE CONTROL EXTERNO (S)
15/04/2019



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

**Resumen Ejecutivo Informe Final N° 92, de 2019
Municipalidad de Bulnes**

Objetivo: Verificar la infraestructura de tecnología de la información, sistemas informáticos y sus respectivos contratos en la Municipalidad de Bulnes, considerando los aspectos relacionados con las licencias del software en uso y su propiedad y el cumplimiento de las políticas, normas, prácticas y procedimientos de control y verificar la observancia de la normativa vigente que rige la materia, especialmente, lo establecido en los decretos supremos N°s. 83 de 2004 y 93 de 2006, ambos del Ministerio Secretaría General de la Presidencia, y del decreto N° 14, de 2014, del Ministerio de Economía, Fomento y Turismo, en lo relativo a normas técnicas sobre mensajes electrónicos masivos no solicitados y sitios electrónicos y plataformas web abiertas, respectivamente.

Preguntas de la Auditoría:

¿Utiliza la Municipalidad de Bulnes servicios de intercambio de información y datos con otras instituciones públicas y/o privadas, a través de interoperabilidad?

¿Cuenta el municipio con las licencias respectivas de los softwares actualmente en uso?

¿Cuenta la repartición con procedimientos destinados a la gestión de la seguridad de la información?

Principales resultados:

- Se observó que la entidad municipal, si bien cuenta con instrucciones sobre la interoperabilidad entre los sistemas institucionales, éstas corresponden a políticas informales, lo que infringe el decreto supremo N° 14 de 2014, del Ministerio de Economía, Fomento y Turismo, que modifica el decreto supremo N°181, de 2002, que Aprueba Reglamento de la ley N° 19.799 sobre Documentos Electrónicos, Firma Electrónica y la Certificación de dicha firma, debiendo el municipio acreditar la creación, formalización e implementación del procedimiento, cuyo avance o término será validado en la etapa de seguimiento.
- Se advirtió que la entidad municipal utiliza distintos programas computacionales en los equipos de los funcionarios, los cuales se encuentran sin su respectiva licencia. Lo expuesto vulnera lo establecido en la letra b), del artículo 22, del decreto supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, sobre gestión de las operaciones y las comunicaciones, de las exigencias relativas al cumplimiento con las licencias de software y la prohibición del uso de software no autorizado, y lo estipulado en los artículos 19 y 20 de la Ley 17.336, sobre Propiedad Intelectual. Al respecto, la municipalidad deberá acreditar la adquisición de las licencias de software, lo que será verificado en la etapa de seguimiento.



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

- Se constató que no existe un manual de descripción de cargos y funciones que indique los lineamientos y permita conocer las tareas, deberes y responsabilidades de los funcionarios que conforman la unidad de informática, lo que no se aviene con lo establecido en el numeral 44, de la resolución exenta N°1.485, de 1996, de la Contraloría General de la República, que señala que una institución debe tener pruebas escritas de su estructura de control interno, incluyendo sus objetivos y procedimientos de control, y de todos los aspectos pertinentes de las transacciones y hechos significativos. Al respecto, la municipalidad deberá remitir la documentación que dé cuenta de la creación de la unidad de informática, informando de ello en un plazo no superior a 60 días hábiles contados de la recepción del presente oficio.
- Se comprobó que, tanto en la gestión municipal como en los servicios traspasados, no se mantiene un inventario actualizado de los bienes que poseen, el cual debiera incluir los activos de información, software y servicios. De igual forma, de las validaciones efectuadas se evidenció que los activos de información carecen de un número, dígito o código que los identifique como tal, conforme a lo recepcionado por antecedentes a través del desarrollo de esta auditoría. Ello infringe lo citado en el numeral 7.1 de la norma NCh-ISO 27.002, de 2009, en cuanto a que la organización deberá identificar todos sus activos y documentar la importancia de ellos, remitiendo la actualización del inventario de bienes y sistemas computacionales. De igual manera tendrá que codificar cada bien con un código de activo fijo que permita identificar dichos bienes, informando de ello en un plazo no superior a 60 días hábiles contados de la recepción del presente oficio.



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

PREG. 37.002/2019
REF N° 400.542/2019

INFORME FINAL N° 92, DE 2019, SOBRE
FISCALIZACIÓN A LAS TECNOLOGÍAS
DE INFORMACIÓN EN LA
MUNICIPALIDAD DE BULNES.

CHILLÁN, - 3 ABR. 2019

En cumplimiento del plan anual de fiscalización de esta Contraloría Regional para el año 2019, y en conformidad con lo establecido en los artículos 95 y siguientes de la ley N° 10.336, de Organización y Atribuciones de la Contraloría General de la República, y 54 del decreto ley N° 1.263, de 1975, Orgánico de Administración Financiera del Estado, se efectuó una fiscalización a las Tecnologías de Información en la Municipalidad de Bulnes, por el periodo comprendido entre el 1 de enero de 2018 y el 11 de febrero de 2019.

El equipo que ejecutó la fiscalización fue integrado por los señores Henry Rodríguez González y David Muñoz Vásquez, fiscalizador y supervisor, respectivamente.

JUSTIFICACIÓN

De los antecedentes tenidos a la vista en la etapa de planificación de las auditorías a realizarse durante el año 2019 y los datos recopilados y analizados por la Unidad Técnica de Control Externo de esta Contraloría Regional, que consideró, entre otros, la información proporcionada por la Contraloría Regional del Biobío y las fechas de las últimas fiscalizaciones efectuadas, se determinó que la Municipalidad de Bulnes se encuentra dentro de las entidades relevantes para ser inspeccionada en materias de tecnologías de información.

A mayor abundamiento, cabe indicar que varios de los municipios de la Región de Ñuble carecen de procesos que aseguren la información y garanticen una continuidad de los servicios asociados. Dicha situación quedó de manifiesto durante el año 2017, toda vez que cuatro de los municipios de la región experimentaron ataques informáticos que afectaron su información contable y presupuestaria, por lo que resulta relevante evaluar el nivel de seguridad de la referida entidad comunal.

Asimismo, a través de esta fiscalización, esta Entidad Superior de Control busca contribuir a la implementación y cumplimiento de los 17 Objetivos de Desarrollo Sostenible, ODS, aprobados por la Asamblea General de las Naciones Unidas en su Agenda 2030, para la erradicación de la pobreza, la protección del planeta y la prosperidad de toda la humanidad.

AL SEÑOR
MARIO QUEZADA FONSECA
CONTRALOR REGIONAL
CONTRALORÍA REGIONAL DE ÑUBLE
PRESENTE



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

En tal sentido, esta revisión se enmarca en el ODS N° 16, Paz, Justicia e Instituciones Sólidas.

ANTECEDENTES GENERALES

La Municipalidad de Bulnes es una corporación de derecho público, con personalidad jurídica y patrimonio propio, cuya finalidad es satisfacer las necesidades de la comunidad local y asegurar su participación en el progreso económico, social y cultural de la comuna, según dispone el artículo 1° de la ley N° 18.695, Orgánica Constitucional de Municipalidades. Dicha entidad está constituida por el alcalde, que es su máxima autoridad, quien ejerce la dirección y administración superior y la supervigilancia de su funcionamiento y por el concejo municipal, órgano colegiado de carácter normativo, resolutivo y fiscalizador, encargado de hacer efectiva la participación de la comunidad local y de ejercer las atribuciones que señala la precitada ley.

Sobre la materia, el decreto supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para los Órganos del Estado sobre la Seguridad y Confidencialidad de los Documentos Electrónicos, en su artículo 1°, establece las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los Órganos de la Administración del Estado, y las demás cuya aplicación se recomienda para los mismos fines.

A su vez, el decreto supremo N° 81 de 2004, de la señalada Cartera de Estado, contiene la norma técnica que establece las características mínimas obligatorias de interoperabilidad que deben cumplir los documentos electrónicos en su generación, envío, recepción, procesamiento y almacenamiento, tanto en los órganos de la Administración del Estado, como en las relaciones de la ciudadanía y el sector privado con dichos órganos, y las demás cuya aplicación se recomienda, las cuales tienen por finalidad asegurar la interoperabilidad en la comunicación de datos; disponer de un marco semántico que asegure la operabilidad entre los diferentes organismos que utilicen documentos electrónicos y su entorno; proveer un mecanismo que permita a los diferentes organismos que utilicen documentos electrónicos, encontrarse, convenir en comunicarse, desarrollar servicios; contar con estándares de repositorios para registro y consulta de funcionalidades de intercambio, y facilitar la consulta por parte de los diferentes órganos de la administración del Estado, de la información que cada uno de ellos mantiene y maneja.

De igual manera, mediante el decreto supremo N° 93 de 2006, del citado Ministerio, se aprueban las normas técnicas para la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los órganos de la Administración del Estado y de sus funcionarios.

Por último, el decreto supremo N° 14, de 2014, del Ministerio de Economía, Fomento y Turismo, modifica el decreto supremo



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

N° 181, de 2002, de ese ministerio, que aprueba el reglamento de la ley N° 19.799, sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.

Enseguida, es oportuno señalar que la citada municipalidad cuenta con un funcionario especialista en informática, quien presta servicios desde el 18 de enero de 2017, según consta en los decretos alcaldicios N°s. 226, 225 y 55, de 2017, 2018 y 2019, respectivamente, cuya dependencia es la Administración Municipal.

Asimismo, es dable señalar que la municipalidad mantiene un contrato de arriendo y mantención de sistemas computacionales con la empresa CAS-CHILE, desde el año 2002, sancionado mediante decreto alcaldicio N° 741, de igual anualidad.

Adicionalmente, cabe indicar que mediante decreto alcaldicio N° 401, de 27 de enero de 2014, se aprobó un trato directo por el servicio de soporte y mantención de software de gestión municipal, pero desde el año 2015 dicho servicio no se encuentra vigente, por faltas reiteradas en dar solución a requerimientos informáticos por parte del proveedor del sistema, la empresa Cybermedia.

El detalle de los módulos se presenta a continuación:

TABLA N° 1: Sistemas contratados y utilizados por la Municipalidad.

CAS-CHILE
Sistema de Contabilidad Gubernamental.
Sistema de Administración de Personal.
Sistema de Remuneraciones.
CIBERMEDIA.
Sistema Permisos de Circulación.
Sistema Ayuda Social.
Sistema Licencias de Conducir.
Sistema Órdenes de Pedido.
Sistema Inventarios.
Sistema Tesorería.
Sistema Recursos Humanos.
Sistema Indicadores Económicos.
CIBERMEDIA.
Sistema Solicitudes Horas Extraordinarias.
Sistema Solicitudes de Viáticos.
Sistema Concejo Municipal.
Sistema Rentas y Patentes.
Sistema Acuerdos de Concejo.
Sistema Tesorería.
Sistema de Publicación de Transparencia Activa.

Fuente: Elaboración propia en base a la información suministrada por el Encargado de Informática de la Municipalidad de Buñes.



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

Además, se debe señalar que el Departamento de Educación Municipal, DAEM, mantiene un contrato de arriendo y mantención de sistemas computacionales con la empresa CAS-CHILE, desde el año 2018, sancionado a través de decreto alcaldicio N° 119, de igual anualidad, y un contrato de arriendo y mantención de sistemas computacionales con la empresa Sistemas Modulares de Computación Limitada, desde 2018, aprobado a través de decreto alcaldicio N° 2.100, del mismo año, según lo que se presenta a continuación:

TABLA N° 2: Sistemas contratados por el DAEM.

SISTEMAS MODULARES COMPUTACIONALES, SMC.
Sistema de Remuneraciones
CAS-CHILE
Sistema de Contabilidad Gubernamental

Fuente: Elaboración propia en base a la información suministrada por el Encargado de Informática de la Municipalidad de Bulnes.

Finalmente, cabe señalar que el Departamento de Salud Municipal, DESAM, también mantiene un contrato de arriendo y mantención de sistemas computacionales con la empresa CAS-CHILE, desde 2018, sancionado a través de decreto alcaldicio N° 78, de 2018 y decreto alcaldicio N° 17, de 2019.

TABLA N° 3: Sistemas contratados por el DESAM.

CAS-CHILE
Sistema de Contabilidad Gubernamental.
Sistema de Administración de Personal.

Fuente: Elaboración propia en base a la información suministrada por el Encargado de Informática de la Municipalidad de Bulnes.

Cabe mencionar que, con carácter confidencial, mediante el oficio N° 454, de 18 de febrero de 2019, fue puesto en conocimiento del Alcalde de la Municipalidad de Bulnes, el Preinforme de Observaciones N° 92, de igual anualidad, con la finalidad de que formule los alcances y precisiones que a su juicio procedieran, lo que se materializó a través del oficio N° 167, de 6 de marzo de 2019, cuyos argumentos y antecedentes de respaldo fueron considerados para la elaboración del presente documento:

OBJETIVO

La fiscalización tuvo por objeto verificar la infraestructura de tecnología de la información, sistemas informáticos y sus respectivos contratos en la Municipalidad de Bulnes, considerando los aspectos relacionados con las licencias de software en uso, su propiedad y el cumplimiento de las políticas, normas, prácticas y procedimientos de control, en el período comprendido entre el 1 de enero de 2018 y el 11 de febrero de 2019.

Lo anterior, con la finalidad de constatar los aspectos que se relacionan con el suministro de información, las políticas, normas, prácticas y procedimientos de control que emanan de dichos procesos, verificando



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

su confiabilidad, seguridad, integridad y disponibilidad de los datos, como la interoperabilidad de los sistemas.

Asimismo, la aludida visita se orientó a verificar el cumplimiento de las disposiciones legales y reglamentarias relativas a la materia.

A su vez, se procedió a evaluar el ambiente de control interno ejercido por la entidad en los procesos auditados, al mes de febrero del año 2019.

METODOLOGÍA

El examen se practicó de acuerdo con la metodología de auditoría de esta Entidad Fiscalizadora, contenida en la resolución N° 20, de 2015, que Fija Normas que Regulan las Auditorías efectuadas por la Contraloría General, y los procedimientos de control dispuestos en la resolución exenta N° 1.485, de 1996, que Aprueba Normas de Control Interno, ambas de este origen, considerando resultados de evaluaciones de control interno respecto de la materia examinada, determinándose la realización de pruebas de fiscalización en la medida que se estimaron necesarias, tales como, análisis documental, validaciones en terreno, entrevistas, entre otros.

Las observaciones que la Contraloría General formula con ocasión de las fiscalizaciones que realiza se clasifican en diversas categorías, de acuerdo con su grado de complejidad. En efecto, se entienden por Altamente Complejas (AC) / Complejas (C) aquellas observaciones que de acuerdo a su magnitud, reiteración, detrimento patrimonial o eventuales responsabilidades funcionarias, son consideradas de especial relevancia por la Contraloría General, en tanto, se clasifican como Medianamente Complejas (MC) / Levemente Complejas (LC), aquellas que tienen menor impacto en esos criterios. Lo anterior, de conformidad con el artículo 52 de la citada resolución N°20, de 2015, donde de acuerdo a la complejidad del hecho observado se determinará la responsabilidad de la validación de su cumplimiento.

Así, los seguimientos que ejecutará esta Entidad Superior de Control, están enfocados, principalmente, en los requerimientos que deriven de observaciones categorizadas como Altamente Complejas (AC) o Complejas (C). Por su parte, la validación de las acciones correctivas que se soliciten respecto a observaciones categorizadas como Medianamente Complejas (MC) y Levemente Complejas (LC), serán de responsabilidad de los Auditores Internos o Encargados de Control Interno de cada entidad pública sujeta a la fiscalización de la Contraloría, esto sin perjuicio de las demás facultades que corresponden a éste Órgano de Control, de conformidad con lo dispuesto en la ley N°10.336, de Organización y Atribuciones de la Contraloría General de la República.

UNIVERSO Y MUESTRA

De acuerdo con los antecedentes proporcionados por la entidad fiscalizada, el universo considerado para este examen



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

incluyó los sistemas basados en tecnologías de información, TI, asociados a la gestión municipal, de los cuales se examinaron sus controles y la revisión de los contratos que dan origen a ellos.

Las partidas sujetas a examen se determinaron analíticamente, revisando para ello un total de 70 equipos computacionales de un universo de 149, informados por la entidad municipal, lo que equivale a un 46,98% del universo antes indicado.

TABLA N° 4: Equipos revisados en la entidad auditada.

MATERIA ESPECÍFICA	UNIVERSO		MUESTRA	
	\$	N°	\$	N°
Equipos Computacionales Municipales.	0	109	0	42
Equipos Computacionales de Educación.	0	31	0	28
Equipos Computacionales de Salud.	0	9	0	0
Total Equipos Computacionales Informados.		149	0	70

Fuente: Elaboración propia en base a la información suministrada por el Encargado de Informática de la Municipalidad de Bulnes.

La información utilizada en la presente auditoría fue proporcionada en el municipio por el Encargado de Informática, la Administradora Municipal, el Jefe (S) del DAEM y el Jefe (S) DESAM; y puesta a disposición de esta Contraloría General, desde el 10 de enero de 2019.

RESULTADO DE LA AUDITORÍA

Del examen practicado, se determinaron las siguientes situaciones:

I. ASPECTOS DE CONTROL INTERNO

Conforme con la citada resolución exenta N°1.485, de 1996, el control interno es un instrumento de gestión que se utiliza para proporcionar una garantía razonable de que se cumplan los objetivos establecidos por la dirección, siendo de su responsabilidad la idoneidad y eficacia del mismo. Así, el director de toda institución pública debe asegurar el establecimiento de una estructura de control adecuada, como también su revisión y actualización permanente a objeto de mantener su eficacia.

En ese contexto, el control interno es un proceso integral efectuado por la máxima autoridad de la entidad y el personal de ésta, para enfrentarse a los riesgos y dar una seguridad razonable de que en la consecución de la misión de la entidad se alcancen: los objetivos institucionales, la ética, eficiencia, eficacia y economicidad de las operaciones; el cumplimiento de las obligaciones de responsabilidad, y las leyes y regulaciones aplicables; y, salvaguardar los recursos para evitar pérdidas, mal uso y daño al patrimonio de la institución.

De la revisión efectuada, se advirtieron las siguientes deficiencias, a saber:



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

1. Omisión de un manual de descripción de cargos y funciones para la Unidad de Informática.

Se constató que no existe un manual de descripción de cargo y funciones que dicte los lineamientos y permita conocer las tareas, deberes y responsabilidades de los funcionarios que conforman la unidad de informática.

Lo anterior no se aviene con lo establecido en el numeral 44, de la citada resolución exenta N° 1.485, de 1996, que señala que una institución debe tener pruebas escritas de su estructura de control interno, incluyendo sus objetivos y procedimientos de control, y de todos los aspectos pertinentes de las transacciones y hechos significativos. Asimismo, la documentación debe estar disponible y ser fácilmente accesible para su verificación al personal apropiado y a los auditores.

Sobre el particular, si bien la municipalidad reconoce lo objetado, corresponde mantener la observación debiendo dicha entidad acreditar la creación, formalización e implementación de la unidad de informática con el respectivo personal a cargo, materia que será verificada en la etapa de seguimiento.

2. Inexistencia de auditorías con un enfoque de Tecnologías de Información.

El municipio no ha realizado auditorías internas o revisiones programadas con un enfoque a las TI, al menos en los últimos 2 años, lo cual fue certificado por el Director de Control Interno con fecha 15 de enero de 2019, señalando que solamente se realizan validaciones a los sistemas propios, internos y externos, con el fin de realizar el cruce de información que permita comprobar la gestión financiera, contable, presupuestaria y administrativa de la municipalidad y sus servicios traspasados.

Lo expuesto, transgrede lo dispuesto en el artículo 38, de la citada resolución exenta N° 1.485, de 1996, el que indica que "Los directivos deben vigilar continuamente sus operaciones y adoptar inmediatamente las medidas oportunas ante cualquier evidencia de irregularidad o de actuación contraria a los principios de economía, eficiencia o eficacia".

De igual forma, el artículo 39 de la referida resolución N° 1.485, de 1996, señala que "La vigilancia de las operaciones asegura que los controles internos contribuyen a la consecución de los resultados pretendidos. Esta tarea debe incluirse dentro de los métodos y procedimientos seleccionados por la dirección para controlar las operaciones y garantizar que las actividades cumplan los objetivos de la organización".

Sobre lo expresado, la entidad no se pronuncia, por lo que mantiene la observación, correspondiéndole al Director de Control del municipio, en lo sucesivo, considerar revisiones sobre la materia examinada.



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

II EXAMEN DE LA MATERIA AUDITADA

1. Falta de manuales de procedimientos formalizados relacionados con la interoperabilidad entre los sistemas institucionales.

Se observó que la entidad municipal, si bien cuenta con instrucciones sobre la materia, descritas por el encargado de informática, estas corresponden a políticas informales relacionadas con la interoperabilidad entre los sistemas institucionales.

De igual forma, se evidencia que el Departamento de Salud no cuenta con una política, plan, instrucción o normativa relacionada con la interoperabilidad entre los sistemas institucionales, lo que fue certificado por el Director de ese departamento.

Por otra parte, el Departamento de Educación no entregó información al respecto.

Sobre lo anterior, cabe indicar que contar con dichos manuales formalizados permite mitigar el riesgo de información inconsistente, así como la simultánea incorporación de los mismos datos en distintos sistemas interdependientes y no integrados.

Lo descrito infringe el decreto supremo N°14 de 2014, del Ministerio de Economía, Fomento y Turismo, que modifica el decreto N°181, de 2002, que Aprueba Reglamento de la ley N° 19.799 sobre Documentos Electrónicos, Firma Electrónica y la Certificación de dicha firma.

Asimismo, transgrede lo establecido en los artículos 3° y 5° de la ley N° 19.880, de Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado, que señalan que las decisiones escritas que adopte la Administración se expresarán por medio de actos administrativos, esto es, decisiones formales emitidas por ellos, en las cuales se contienen declaraciones de voluntad, realizadas en el ejercicio de una potestad pública, las cuales deben efectuarse por escrito.

Al respecto, el municipio informa que se elaborará y formalizará el manual de procedimientos señalado.

Sobre lo expuesto, se debe mantener lo observado y esa entidad municipal deberá acreditar la creación, formalización e implementación del procedimiento relacionado con la interoperabilidad entre sistemas institucionales e informar de ello a los distintos directores de departamentos, cuyo avance o término se analizará en la etapa de seguimiento.

2. Sobre políticas de asignación de cuentas de usuario y claves de acceso.

a) Se observa que la entidad municipal, si bien cuenta con instrucciones descritas por el informático, para crear, definir y asignar las contraseñas temporales, para que los usuarios ingresen por primera vez



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

a los sistemas en revisión, estas no se encuentran formalizadas a través de un decreto alcaldicio.

Además, se verificó que el Departamento de Salud no cuenta con una política, plan, instrucciones o normativa relacionada para crear, definir y asignar las contraseñas temporales, lo que fue ratificado mediante certificado del director del departamento.

Por último, el DAEM, no proporcionó información al respecto, por lo que no consta la existencia de dichas políticas.

Lo descrito infringe lo indicado en los artículos 28 letra j) y 29, del decreto supremo N° 83 de 2004, del Ministerio Secretaría General de la Presidencia, en concordancia con el acápite 11.2.3, letras b), c), d) y e), de la norma NCh-ISO N° 27.002, de 2009.

En este sentido, es oportuno destacar que, según lo ha reconocido la jurisprudencia administrativa -contenida en los dictámenes N°s 31.870, de 2010 y 10.449, de 2011, entre otros- y en armonía con el principio de escrituración que rige los actos de la Administración del Estado, consagrado en el artículo 5° de la aludida ley N° 19.880, las decisiones que adopten las municipalidades deben materializarse en un documento por escrito y aprobarse a través de decreto alcaldicio, por lo que la expresión formal de la voluntad de la entidad edilicia, sólo puede perfeccionarse con la expedición del respectivo acto administrativo, siendo éste el que produce el efecto de obligar al municipio conforme a la ley, lo que no ocurre en la especie.

b) Se observó que la entidad municipal no cuenta con los procedimientos relacionados con la revisión de intervalos frecuentes de los permisos de acceso de los usuarios, políticas de claves en cuanto a la periodicidad o caducidad, puesto que son indefinidas y la falta de un encargado de revisión de dichos procesos.

Lo expuesto, vulnera lo señalado en el punto 11.2.4, la mencionada NCh-ISO 27.002, de 2009, sobre revisión de derechos de acceso de usuario, el cual indica que "La dirección deberá revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal".

Tampoco se ajusta a lo exigido en la letra h), del artículo 28 del decreto supremo N° 83 de 2004, Ministerio Secretaría General de la Presidencia, respecto a que los identificadores deben ser cambiados en intervalos regulares.

c) Se advirtió que la entidad edilicia, si bien cuenta con instrucciones respecto de las obligaciones, prohibiciones, recomendaciones e indicaciones para la selección y uso de contraseñas, éstas no se encuentran formalizadas por un decreto alcaldicio, ya que son solo directrices efectuadas por el encargado de informática.



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

Adicionalmente, a través de un certificado del Director (S) del DESAM, éste informó que no cuentan con estas políticas.

Por último, el DAEM no entregó información sobre la materia, por lo que no consta la existencia de este tipo de instrucciones.

Lo expuesto, infringe lo establecido en las letras a) a j), del artículo 28 del decreto N° 83 de 2004, Ministerio Secretaría General de la Presidencia, respecto a que los identificadores deben ser cambiados en intervalos regulares, en concordancia con el acápite 11.2.3, letras b), c), d) y e), de la norma NCh-ISO N° 27.002, de 2009.

Asimismo, transgrede lo indicado en el artículo 3° de la aludida ley N° 19.880, en cuanto a que las decisiones escritas que adopte la Administración se expresarán por medio de actos administrativos.

d) En relación a la existencia de un procedimiento formal para registrar la otorgación o revocación de los permisos de acceso a los sistemas de información, se verificó que no existe tal documento, lo que vulnera lo indicado en el punto 11.2.1, de la citada norma NCh 27.002, de 2009, la cual señala que "Deberá existir un procedimiento formal de registro y cancelación de registro para otorgar y revocar los accesos a todos los servicios y sistemas de información". Ello, conforme a lo indicado por la administradora municipal y el Director de Salud, en certificados entregados a este Organismo Fiscalizador.

En su respuesta la municipalidad menciona que respecto las letras a), b) y c) de este título, creará y decretará los documentos que contengan las Políticas de Acceso a los Sistemas de Información Municipales y las Políticas de Gestión y Uso de Contraseñas para sistemas de Información Municipales. No obstante, sobre la letra d), no se pronuncia.

En atención a lo expuesto, corresponde mantener la observación mientras no se verifique por parte de esta Entidad de Control, la creación, formalización e implementación de los procedimientos citados, materia cuyo avance será validado en la etapa de seguimiento.

3. Sobre la existencia y utilización de políticas, planes o procedimientos formalizados sobre uso, almacenamiento, acceso y distribución de mensajes electrónicos

Se observó que tanto en las áreas de Gestión Municipal como el DAEM y el DESAM, no se cuenta con una política, plan, o normativa relacionada con instrucciones sobre uso, almacenamiento, acceso y distribución de mensajes electrónicos, lo que fue ratificado por la administradora municipal y los directores de Educación y Salud.

Lo anterior infringe lo indicado en la letra b), del artículo 2 del decreto supremo N° 93 de 2004, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica para la Adopción de Medidas Destinadas a Minimizar los Efectos Perjudiciales de los Mensajes Electrónicos



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

Masivos no Solicitados Recibidos en las Casillas Electrónicas de los Órganos de la Administración del Estado y de sus Funcionarios.

Sobre la materia, la entidad expone que creará un reglamento que establezca el uso del correo electrónico y el uso del servicio de internet municipal.

En cuanto a lo informado, corresponde mantener la observación, mientras no se acredite la creación, formalización e implementación del reglamento de uso del correo electrónico y de servicios de internet municipal, cuyo avance o término será verificado en la etapa de seguimiento.

4. Ausencia de un plan de contingencia institucional.

Se observó que la entidad no cuenta con un plan de contingencia que permita asegurar la continuidad de los sistemas que aportan sus operaciones críticas, conforme fue mencionado por el Encargado de Informática del municipio y certificado por la Administradora Municipal.

Lo anterior infringe lo indicado en el artículo 35 del citado decreto supremo N° 83 de 2004, del Ministerio Secretaría General de la Presidencia, que se refiere a que "el encargado de seguridad deberá formular un plan de contingencia para asegurar la continuidad de operaciones críticas para la institución. Este plan deberá, como mínimo, disponer la efectiva gestión de las relaciones públicas, la eficiente coordinación con las autoridades apropiadas, como policía, bomberos, autoridades directivas, etc., y mecanismos eficaces para convocar a quienes sean los responsables de los documentos electrónicos y sistemas informáticos afectados".

De igual forma se vulnera lo indicado en el numeral 14.1.3, de la Norma Chilena NCh-ISO 27.002, de 2009, referida a Tecnologías de la Información, del Instituto Nacional de Normalización, en cuanto a que "se deberán desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requeridos, después de la interrupción o la falla de los procesos críticos para el negocio".

En su respuesta la municipalidad señala que luego del nombramiento del encargado de seguridad de la información, este tendrá que crear el plan de contingencia institucional, agregando que la implementación de la infraestructura de soporte para este plan quedará sujeta a la disponibilidad de recursos financieros.

Al respecto, se debe mantener la observación debiendo ese municipio acreditar la confección, formalización e implementación del plan de contingencia, que permita asegurar la continuidad de los sistemas que aportan sus operaciones críticas, cuyo avance o término será validado en la etapa de seguimiento.



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

5. Sobre procedimientos para resguardar la confidencialidad de la información.

Se observó que el DAEM y el DESAM no cuentan con una política, plan, instrucciones o normativa de contingencia informática que permitan resguardar la confidencialidad de la información que administra la entidad en los sistemas de información, conforme a lo mencionado por los directores de Educación y Salud.

Lo anterior infringe lo indicado en el numeral 46 de la citada resolución exenta N° 1.485, de 1996, la cual se refiere a que "la documentación sobre transacciones y hechos significativos debe ser completa y exacta, permitiendo facilitar el seguimiento de la transacción o hecho antes, durante y después de su realización".

De igual forma, vulnera lo indicado en el artículo 6, del decreto supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, referido a la seguridad del documento electrónico en general (confidencialidad, integridad, factibilidad de autenticación, y disponibilidad).

Sobre lo expuesto, la municipalidad no se pronuncia, por lo que la observación se mantiene, correspondiéndole a esa entidad confeccionar, formalizar e implementar los procedimientos necesarios que permitan contribuir al resguardo de la confidencialidad de la información que administran, materia cuyo avance o término será validado en la etapa de seguimiento.

6. Falta de política de seguridad de la información.

Se observó que en el área municipal, el DAEM y el DESAM, no existe un procedimiento formalizado que fije el tratamiento de la entidad para gestionar la seguridad de la información, tanto para los sistemas propios, de terceros, como de aquellos con los que interoperan, conforme a lo informado tanto por la Administradora Municipal y los Directivos de Educación y Salud.

Lo expuesto, infringe lo señalado en el artículo 11 del señalado decreto supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, el cual indica que "deberá establecerse una política que fije las directrices generales que orienten la materia de seguridad dentro de cada institución, que refleje claramente el compromiso, apoyo e interés en el fomento y desarrollo de una cultura de seguridad institucional".

De igual forma "La política de seguridad deberá incluir, como mínimo, lo siguiente: a) Una definición de seguridad del documento electrónico, sus objetivos globales, alcance e importancia. b) La difusión de sus contenidos al interior de la organización. c) Su reevaluación en forma periódica, a lo menos cada 3 años. Las políticas de seguridad deberán documentarse y explicitar la periodicidad con que su cumplimiento será revisado".

En su respuesta, el municipio informa que el encargado de seguridad de la información creará la reglamentación sobre las



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

políticas generales de un sistema de gestión de seguridad de la información y la clasificación y manejo de la información, las que serán revisadas y aprobadas por el comité de seguridad de la información y aprobada por alcaldía.

En cuanto a lo informado por la municipalidad, corresponde mantener la observación, mientras no se verifique la elaboración, formalización e implementación del procedimiento relacionado con las políticas de seguridad de la información en el municipio, lo que será revisado en la etapa de seguimiento.

7. Inexistencia de procedimientos de respaldo de la información.

Se observó que el DAEM y el DESAM, no cuentan con un procedimiento escrito y formalizado referido a la realización de copias de seguridad de la información de sus sistemas informáticos, lo que fue ratificado por los directores de los departamentos singularizados.

Lo expuesto, no se ajusta al artículo 37, letra f), del decreto supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, que dispone que se aplicarán las normas del capítulo 8, de la NCh 2.777, del año 2003, reemplazada por el capítulo 10, de la mencionada norma NCh-ISO 27.002, de 2009, el cual manifiesta que se deben establecer todas las responsabilidades y procedimientos para la gestión y operación de todas las instalaciones de procesamiento de información. Esto incluye el desarrollo de procedimientos operativos apropiados.

En cuanto a lo señalado, la municipalidad no aporta explicaciones, por lo que se mantiene íntegramente la observación, debiendo esa entidad edilicia desarrollar, formalizar e implementar los procedimientos que permitan establecer los parámetros y medidas para la realización de las copias de seguridad de la información que manejan los sistemas informáticos, materia que será verificada en la etapa de seguimiento.

8. Falencias en la sala de servidores.

De la revisión efectuada a los racks en donde se encuentran los servidores computacionales de la Gestión Municipal y DAEM, el 10 de enero de 2019, se observaron las siguientes situaciones:

- a) No existen salas de servidores.
- b) Actualmente el rack de los servidores del municipio se encuentra a un lado de la caja de tesorería, lugar de libre acceso y circulación que como única medida de seguridad, cuenta con una cámara fotográfica con sensor de detección de movimiento.
- c) El rack de comunicaciones del municipio se encuentra en el Edificio de la Cultura, al lado de una sala de eventos bajando unas escaleras de libre tránsito y acceso al público.



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

d) Actualmente los racks del servidor y de comunicaciones del DAEM se encuentran en el segundo piso de las dependencias, en un sector de fácil acceso de todo el personal.

De lo expuesto, se constató que no se dispone de medidas de protección, tales como perímetro de seguridad, sensores para humo, temperatura, humedad, extintor, equipos de aire acondicionado y apertura de puertas, de forma tal de evitar eventuales robos y pérdidas de información. Adicionalmente, no se publicitan las instrucciones relativas a la prohibición del consumo de alimentos, bebidas y tabaco en las cercanías de los sistemas informáticos y no existe un registro de todas las visitas autorizadas a la sala de servidores. El detalle se presenta en el anexo N° 1, del presente informe.

Todo lo expuesto vulnera los artículos 17, respecto a la protección física de los equipos a las amenazas de riesgos del ambiente externo; 18 letra b), sobre las condiciones climatológicas y ambientales que pueden afectar los sistemas informáticos; y 37, letra e), del decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, el cual establece que se aplicará la sección 7.1, del capítulo 7 de la norma NCh 2.777, del año 2003, la que debe entenderse referida al punto 9.1 de la norma NCh-ISO 27.002, de 2009, que especifica que las instalaciones de procesamiento de información crítica o sensible de la organización deberán estar ubicadas en áreas seguras, sólidas y resguardadas por un perímetro de seguridad definido, con barreras de seguridad y controles de acceso apropiados.

Además, se reafirma en el numeral 9.2.1 de la norma NCh-ISO 27.002, de 2009, que expresa, con respecto a la ubicación y protección del equipamiento, se deberá ubicar o proteger para reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizados.

e) Se evidenció que la entidad auditada no ha desarrollado un procedimiento para autorizar y registrar los ingresos y salidas de personal externo, revisar y modificar periódicamente los derechos de acceso y la obligación de autorizar y supervisar todos los trabajos realizados por personal externo en la sala de servidores. Tal carencia incumple el literal e), del artículo 37 del decreto N° 83 de 2004, del citado Ministerio, y el acápite 9.1.2, letras a), d) y e) de la NCh-ISO 27.002, de 2009.

En su respuesta el municipio indica que realizará las gestiones para adquirir e instalar mamparas de protección con puerta de acceso y llave, que dispondrá de elementos de protección física contra robo e incendios, todo lo cual contará con su debida señalización, instrucciones y advertencias, para los lugares donde se encuentran los racks de telecomunicaciones y donde se trasladará el rack de servidores ubicado en el Edificio de la Cultura.

Agrega que desarrollará un sistema de registro de acceso a la sala de servidores y a los racks telecomunicaciones.



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

Sobre el particular, si bien la entidad informa las acciones a ejecutar, éstas no permiten desvirtuar lo objetado, por lo que se mantiene la observación mientras no se verifique la implementación de las medidas comprometidas respecto de la sala de servidores del municipio, lo que será corroborado en la etapa de seguimiento.

9. Sobre segregación de funciones en los sistemas computacionales.

Se observó que el DESAM y el DAEM no poseen una política de segregación de funciones en los sistemas, considerando que cada cuenta debe estar asociada a las labores que cumple un funcionario, lo cual infringe el artículo 23, del referido decreto supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, el que menciona que "Para los efectos de reducir el riesgo de negligencia o mal uso deliberado de los sistemas, deberán aplicarse políticas de segregación de funciones. Asimismo, deberán documentarse los procedimientos de operación de sistemas informáticos e incorporarse mecanismos periódicos de auditorías de la integridad de los registros de datos almacenados en documentos electrónicos".

Lo expuesto, tampoco se ajusta a lo establecido en el numeral 10.1.3 de la norma NCh 27.002 de 2009, la cual señala que "Se deberán segregar las tareas y las áreas de responsabilidad para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización".

Sobre lo expuesto el municipio no se pronuncia, por lo que se debe mantener la observación, mientras no se verifique la existencia de medidas y acciones orientadas a asegurar la debida segregación de funciones, con el fin de disminuir el riesgo de acceso a los sistemas por distintas personas.

10. Deficiencias relacionadas con las características de las contraseñas.

a) Sobre la materia, en el DAEM, se observó que dos claves de acceso a los sistemas no cumplen con las características mínimas de ocho caracteres, alfanuméricos, no consecutivos ni idénticos y difíciles de recordar, lo cual infringe lo establecido en la letra g), de los artículos 28 y 37, del señalado decreto supremo N° 83, de 2004, Ministerio Secretaría General de la Presidencia. El detalle se presenta a continuación:

TABLA N° 5: Deficiencias en contraseñas encontradas.

RUN	NOMBRE FUNCIONARIO	USUARIO	CONTRASEÑA
12.976.467-8	María San Martín Márquez.	sanmartín	██████
18.746.475-7	Daniela Poza Sepúlveda.	Cvivallos	██████████

Fuente: Elaboración propia en base a la información suministrada por el Encargado de Informática de la Municipalidad de Bulnes.



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

Al respecto, la letra g) del artículo 28 del aludido decreto, recomienda elegir identificadores que tengan una longitud mínima de 8 caracteres; sean fáciles de recordar; contengan letras, mayúsculas, dígitos y caracteres de puntuación; no estén basados en cosas obvias o de fácil deducción a partir de datos relacionados con la persona; estén libres de caracteres idénticos consecutivos o grupos completamente numéricos o alfabéticos; y, no sean palabras de diccionario o nombres comunes.

Asimismo, el numeral 11.3 de la norma NCh-ISO 27.002, de 2009, señala que "se debe prevenir el acceso de usuarios no autorizados, y el robo o compromiso de la información y de las instalaciones de procesamiento de datos, exigiendo a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas".

b) Por otra parte, es dable advertir que, respecto a la gestión municipal, no fueron entregados los antecedentes asociados a las contraseñas utilizadas en sus diversos sistemas y funcionarios, por lo cual no se pudo acreditar el cumplimiento de las normas citadas previamente, situación que la entidad comunal deberá informar documentadamente.

En su respuesta la municipalidad menciona, en síntesis, que se creará una política de gestión y uso de contraseñas para los sistemas de información municipales, la que contendrá los mecanismos de control de cumplimiento de estas normas.

Por otra parte, indica que los sistemas de gestión web municipales, serán reemplazados el presente año, según planificación, debido a su antigüedad y las múltiples deficiencias que poseen en su funcionalidad y seguridad.

Agrega que con el fin de cumplir el requerimiento de este Organismo de Control, se coordinará la creación de un archivo con todas las contraseñas en uso al momento del requerimiento y con expresa instrucción a los funcionarios de que una vez informadas por escrito, cada funcionario debe cambiar dicha contraseña.

Concluye señalando que se informará a aquellos funcionarios cuyas contraseñas no cumplan el estándar, para que las cambien conforme a las recomendaciones antes mencionadas.

Respecto a lo expuesto por el municipio, corresponde mantener la observación mientras no se verifique la elaboración, formalización e implementación del reglamento de uso de contraseñas y demás medidas señaladas en su respuesta.

Adicionalmente, la entidad edilicia deberá mantener un registro de las contraseñas del personal y asegurar que estas cumplan con las exigencias establecidas en la normativa citada en el presente numeral.



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

La verificación de todas las medidas descritas, será efectuada en la etapa de seguimiento.

11. Sobre las casillas electrónicas de los funcionarios.

De las 98 casillas de correos electrónicos revisadas, se constató que en la página web de la entidad auditada, <http://imb.cl/alcalde/>, se difunden 14 casillas de correos electrónicos institucionales, en formato texto, lo que vulnera lo establecido en el artículo 6°, del decreto N° 93, de 2006, del Ministerio Secretaría General de la Presidencia, el cual dispone, en lo que interesa, que cuando fuese necesario difundir las casillas institucionales, los Órganos de la Administración del Estado deben optar por la inclusión de una imagen con la dirección electrónica, el ofuscamiento de ésta, o su despliegue mediante la ejecución de un script por parte de quien la requiera.

TABLA N° 6: Casillas de correo electrónico sin tratamiento de ofuscamiento.

UNIDAD	EMAIL ADDRESS
Director de Control Interno.	control@imb.cl
Director Administración y Finanzas.	daf@imb.cl
Secretaría Administración Municipal.	sec.administracion@imb.cl
Secretaría Alcaldía.	sec.alcaldia@imb.cl
Secretaría Desarrollo Económico Local.	sec.del@imb.cl
Secretaría Desarrollo Social.	sec.dideco@imb.cl
Secretaría Departamento de Obras Municipales.	sec.dom@imb.cl
Secretario Municipal.	sec.municipal@imb.cl
Secretaría Dirección de Tránsito.	sec.transito@imb.cl
Secretaría Secretaría de Planificación.	secre.secplan@imb.cl
informaciones	contacto@imb.cl
Secretaría Dirección de Educación Municipal.	sec.daem@imb.cl
Secretaría Juzgado Policía Local.	sec.jpl@imb.cl
Secretaría Dirección de Salud Municipal.	sec.desamu@imb.cl

Fuente: Elaboración propia en base a la información suministrada por el Encargado de Informática de la Municipalidad de Bulnes.

La municipalidad señala, en su respuesta, que se instruirá al encargado de informática actualizar los contenidos del sitio web municipal, con el motivo de eliminar la información de casillas de correo institucional mostradas en formato texto y las reemplace por imágenes que muestren dichas direcciones, con el fin de evitar la inclusión automatizada de éstas en bases de datos de terceros.

Sobre lo expuesto, si bien las medidas informadas por el municipio resultan atingentes, corresponde mantener la observación mientras no se verifique la implementación de lo mencionado, con el fin de dar cumplimiento al artículo 6°, del decreto supremo N° 93, de 2006, Ministerio Secretaría General de la Presidencia, lo que será verificado en el seguimiento del presente informe.



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

12. Sobre la existencia de un oficial y comité de seguridad.

La municipalidad no cuenta con un oficial o comité de gestión de la seguridad de la información, según lo indicado mediante certificados entregados por el área de Gestión Municipal y sus servicios traspasados, lo que imposibilita, entre otros aspectos, emitir lineamientos para la gestión de la seguridad de la información, revisar y aprobar las políticas de seguridad; conocer los riesgos a los cuales se encuentran expuestos los activos de información; revisar o analizar los incidentes de seguridad; y aprobar iniciativas para mejorar las operaciones informáticas.

Lo anterior, vulnera lo establecido en el artículo 12, del antes citado decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, sobre la seguridad organizacional, que indica que en cada organismo regido por esta norma deberá existir un encargado de seguridad, que actuará como asesor del jefe de servicio correspondiente en las materias relativas a seguridad de los documentos electrónicos. Las funciones específicas que desempeñe internamente el encargado de seguridad serán establecidas en la resolución que lo designe. En todo caso, deberá ejercer, a lo menos, las siguientes funciones:

- a) Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de su organización y el control de su implementación, además de velar por su correcta aplicación.
- b) Coordinar la respuesta a incidentes computacionales.
- c) Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.

De igual forma, el acápite 6.1.1, de la norma NCh-ISO 27.002, de 2009, ya citada, indica que la dirección deberá apoyar activamente la seguridad dentro de la organización a través de una orientación clara, compromiso demostrado, y la asignación explícita de las responsabilidades de seguridad de la información y su reconocimiento. Asimismo, el acápite 6.1.2, señala que las actividades referentes a la seguridad de la información deberán ser coordinadas por representantes de diferentes partes de la organización con funciones y roles pertinentes.

El municipio expone que se conformará el comité respectivo y se formalizará el nombramiento de un funcionario como encargado de seguridad de la información.

Ante lo expuesto, procede mantener lo observado hasta que se acredite la creación, designación y formalización del comité de seguridad de la información, cuyo avance o término será validado en la etapa de seguimiento.



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

13. Sobre los inventarios de hardware y software.

Se constató que tanto en la gestión municipal como en los servicios traspasados no se mantiene un inventario actualizado de los bienes que poseen, el cual deberá incluir los activos de información, software y servicios. De igual forma, de las validaciones efectuadas se evidenció que los activos de información no poseen un número, dígito o código que los identifique como tal, conforme a lo recepcionado por antecedentes a través del desarrollo de esta auditoría.

Lo expuesto, infringe lo citado en el numeral 7.1 de la norma NCh-ISO 27.002, de 2009, en cuanto a que la organización deberá identificar todos sus activos y documentar la importancia de ellos. El inventario de activos deberá incluir toda la información necesaria en caso de tener que recuperar el activo luego de un desastre. Esto incluye tipo de activo, formato, localización, información del respaldo, información de licencias e importancia para el negocio, además, éste inventario no deberá duplicar innecesariamente otros inventarios, pero sí garantizar que el contenido esté alineado.

En su respuesta el municipio indica que instruirá a los encargados de inventario de cada departamento municipal y al jefe general, para que procedan a actualizar el registro de bienes y activos informáticos.

Agrega que, durante esta anualidad, entre otros, se reemplazará el sistema informático de inventarios por uno nuevo, por lo que se migrará la información y se le asignará código único a todos los bienes y activos informáticos municipales, etiquetándolos en cada dependencia donde se encuentran.

Sobre lo expuesto, si bien la entidad informa las medidas para actualizar el inventario de bienes, corresponde mantener la observación, por lo que la municipalidad deberá dar cumplimiento a lo señalado, actualizando el inventario de software y hardware, acreditando las identificaciones respectivas, lo que será verificado en la etapa de seguimiento.

14. Sobre el licenciamiento, disponibilidad y pago del software de la repartición.

a) Sobre la materia, se observó que la entidad municipal utiliza distintos programas computacionales en los equipos de los funcionarios, cuyo detalle se encuentra en anexo N° 2, los cuales se encuentran sin su respectiva licencia.

Lo expuesto vulnera lo establecido en la letra b), del artículo 22, del decreto supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, sobre gestión de las operaciones y las comunicaciones, de las exigencias relativas al cumplimiento con las licencias de software y la prohibición del uso de software no autorizado, y lo estipulado en los artículos 19 y 20 de la ley N° 17.336, sobre Propiedad Intelectual, que disponen que nadie podrá utilizar públicamente una obra del dominio privado sin haber obtenido la autorización expresa del titular del derecho de autor. La infracción de lo dispuesto en este artículo



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

hará incurrir al o los responsables en las sanciones civiles y penales correspondientes.

b) Por otra parte es dable señalar que, la utilización de la versión del software antivirus AVAST Free que, en cuanto a seguridad otorgada, es insuficiente para cumplir los estándares de seguridad informáticas actuales. Ello se ve expresado en la inexistencia de cobertura en contra de los llamados Ransomware, lo que constituye un riesgo operacional, ya que cualquier vulneración de su seguridad impediría la continuidad de los servicios de la repartición y va en contra de lo expresado en materias de seguridad de la información en el artículo 11 del mencionado decreto supremo N° 83, de 2004 y NCh-ISO N° 27.002, de 2009; numeral 10.4, que hace referencia a proteger la integridad del software y de la información, donde se requieren ciertas precauciones para prevenir y detectar la introducción de código malicioso y código móvil no autorizado, además del numeral 10.4.1, y en particular la letra d), donde se indica que la instalación y actualización regular de antivirus para detección y reparación de software que exploren los computadores y los soportes de forma rutinaria o como un control preventivo.

En su respuesta la municipalidad adjunta instrucciones enviadas por la administración municipal y por el encargado actual de informática, a través de correo electrónico, a todos los directores de los departamentos municipales y funcionarios, mediante el cual se prohíbe la instalación de software ilegal en computadores de la entidad.

Agrega que se solicitó formalmente y en diversas oportunidades a los directores y funcionarios que comunicaran las necesidades de software para el desarrollo de sus trabajos. Además, respecto de los equipos que aparecen en la observación, se analizará cada caso verificando si se trata de software gratuito, no actualizado o definitivamente de software de pago instalado ilegalmente por los funcionarios, caso este último en que se instruirá la realización de sumarios administrativos a quienes los usan y sean responsables de los equipos, según instrucciones que se han dado con anterioridad.

Finalmente, respecto del antivirus, informa que se está cotizando dicho servicio a través de una licencia pagada que se instalará en los equipos computacionales del municipio.

En cuanto a lo expuesto, si bien se aceptan las medidas informadas, se debe mantener lo observado, hasta que la municipalidad acredite la utilización y adquisición de licencias de softwares autorizadas y que cumplan con lo establecido en la ley N° 17.336, sobre Propiedad Intelectual.

De igual forma tendrá que adoptar las medidas para supervisar o vigilar la instalación de softwares no autorizados en los equipos institucionales.

Por último, deberá informar los resultados de las validaciones en los equipos observados, adjuntando la documentación de respaldo pertinente, aspectos que serán verificados en la etapa de seguimiento.



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

15. Sobre la existencia de los respaldos, en cuanto a periodicidad, integridad, acceso y un centro de respaldo alternativo.

El DAEM y el DESAM, no proporcionaron antecedentes asociados a la realización de respaldos de información, lo que además queda demostrado por la inexistencia de procedimientos asociados formalizados.

Lo expuesto, infringe lo citado en el artículo 24, del decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, en el cual establece que en los órganos regidos por la presente norma, deberán realizarse copias de respaldo de la información y las aplicaciones críticas para la misión de la institución en forma periódica, en conformidad con las siguientes reglas expresadas en las letras a) a la g).

Además, en el numeral 10.5.1 de la norma NCh-ISO 27.002, de 2009, se señala con respecto al respaldo de la información, que se deberán crear copias de seguridad de la información y del software, probándose regularmente, acorde con la política de respaldo.

Sobre lo expuesto el municipio no se pronuncia, por lo que corresponde mantener la observación, debiendo esa entidad crear, formalizar e implementar un procedimiento de respaldo de la información y acreditar que la documentación que manejan los sistemas de información de los servicios traspasados del municipio cuentan con las copias de seguridad respectivas, lo que tendrá que demostrarse en la etapa de seguimiento.

16. Sobre incidente de seguridad en visita a terreno.

En visita efectuada el 10 de enero del presente año, a los distintos servidores que mantiene el municipio, se constató un incidente de seguridad que se menciona a continuación:

Durante el transcurso de las validaciones, se informa al encargado de informática sobre la existencia de un problema de comunicaciones que estaría afectando el acceso de los usuarios a los sistemas internos, por lo que el profesional verificó el servicio de conexión interna desde el DNS y, efectivamente, este no respondía.

Ante tal situación se procedió a verificar la conexión del router con la fibra de la empresa proveedora, se comprobó que estaba desconectada a la Uninterruptible Power System, UPS, -Sistema de Energía Ininterrumpida-.

En su respuesta, el municipio indica que respecto de las fallencias en algunos puntos críticos de las instalaciones de infraestructura de red de datos y eléctrica, así como el respaldo de estas, se realizarán las adecuaciones que sean pertinentes para subsanar las vulnerabilidades, se creará una política de gestión y acceso a la red municipal, junto con implementar un mini centro de monitoreo de la red LAN.



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

De acuerdo a lo expuesto, se debe mantener la observación, debiendo la entidad acreditar, en lo sucesivo, la solución de las falencias detectadas en la revisión de este Organismo de Control y que pueden afectar los sistemas de información que manejan.

17. Sobre pérdida de información en el computador del Director del Departamento de Educación.

Al respecto, es dable indicar que se constató que el señor Hary Donoso López, Jefe (S) del Departamento de Educación Municipal, informó a través de memorándum N° 4, de 2019, que al asumir funciones el 10 de diciembre de 2018, el equipo computacional asignado no contenía ningún registro de archivos ni información, por lo que solicitó la revisión del computador por parte del encargado de informática del municipio, quien constató la inexistencia de información.

Sobre lo expuesto, el numeral 15.1.3 de la norma NCh-ISO 27.002, de 2009, referida a Tecnologías de la Información, del Instituto Nacional de Normalización, sobre Protección de los Registros de la Organización, señala que se deben proteger los registros importantes de la organización frente a su pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, regulatorios, contractuales y del negocio.

Sobre este punto la municipalidad no se pronuncia, por lo que se mantiene íntegramente la observación, correspondiéndole a la entidad, en lo sucesivo, respaldar la información que se maneja en los sistemas informáticos, tal como se señaló en el numeral 15 de este acápite. De igual forma, corresponde coordinar e informar al funcionario encargado de informática sobre la desvinculación del personal, con el fin de resguardar la documentación existente en los equipos computacionales.

CONCLUSIONES

Atendidas las consideraciones expuestas durante el desarrollo del presente trabajo, la Municipalidad de Bulnes ha aportado antecedentes e iniciado acciones que no han sido suficientes para subsanar las situaciones planteadas en el Preinforme de Observaciones N° 92, de 2019, de esta Contraloría Regional, por lo que se mantienen todas las observaciones, correspondiéndole a la entidad adoptar medidas con el objeto de dar estricto cumplimiento a las normas legales y reglamentaria que las rigen, entre las cuales se estima necesario considerar, a lo menos las siguientes:

1. En cuanto a lo representado en el acápite I, sobre Control Interno, numeral 1, relacionado con la omisión de un manual de descripción de cargos y funciones para la Unidad de Informática, procede que la entidad municipal acredite la confección, formalización e implementación de dicho manual y la creación del departamento de informática, cuyo avance o término se analizará en la etapa de seguimiento (MC).



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

2. Sobre lo expuesto en el acápite I, sobre Control Interno, numeral 2, relacionado con la inexistencia de auditorías con un enfoque de tecnologías de información, el municipio deberá en lo sucesivo considerar en su plan anual de auditorías, revisiones sobre la materia examinada, cuyo avance o término se analizará en la etapa de seguimiento (MC).

3. En lo relacionado al acápite II, sobre Examen de la Materia Auditada, numeral 1, relativo a la falta de manuales de procedimientos formalizados relacionados con la interoperabilidad entre los sistemas institucionales, la municipalidad deberá elaborar, formalizar e implementar el manual de procedimientos, debiendo informar a las distintas jefaturas de dicho documento, materia que será validada en el seguimiento del informe (MC).

4. Sobre lo indicado en el acápite II, Examen de la Materia Auditada, numeral 2, letras a), b), c) y d), acerca de políticas de asignación de cuentas de usuario y claves de acceso, esa entidad edilicia deberá desarrollar, formalizar e implementar los procedimientos sobre la asignación de cuentas de usuario y las claves de acceso de los funcionarios en los distintos sistemas de información que maneja la municipalidad, lo que será validado en la etapa de seguimiento del presente informe (MC).

5. Sobre lo expuesto en el acápite II, Examen de la Materia Auditada, numeral 3, relacionado con la existencia y utilización de políticas, planes o procedimientos formalizados sobre uso, almacenamiento, acceso y distribución de mensajes electrónicos, la municipalidad tendrá que desarrollar, formalizar e implementar el reglamento que permita el correcto uso del correo electrónico y de servicios de internet municipal, materia que será verificada en la etapa de seguimiento (MC).

6. Al tenor de lo consignado en el acápite II, Examen de la Materia Auditada, numeral 4, sobre la ausencia de un plan de contingencia institucional, el municipio deberá elaborar, formalizar e implementar el plan de contingencia que permita asegurar la continuidad de las operaciones críticas para la institución, lo que será verificado en la etapa de seguimiento (MC).

7. Sobre lo mencionado en el acápite II, Examen de la Materia Auditada, numeral 5, relativo a los procedimientos para resguardar la confidencialidad de la información, esa entidad comunal tendrá que elaborar, formalizar e implementar el procedimiento que permita establecer los mecanismos necesarios para resguardar la confidencialidad de la información que maneja el municipio en los sistemas de información, cuyo avance o término se analizará en la etapa de seguimiento (MC).

8. En cuanto a lo señalado en el acápite II, Examen de la Materia Auditada, numeral 6, sobre política de seguridad de la información, la municipalidad deberá crear, formalizar e implementar el procedimiento que contenga las directrices generales que instruyan sobre seguridad de información en la institución, cuyo avance o término se analizará en la etapa de seguimiento (MC).



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

9. Acerca de lo anotado en el acápite II, Examen de la Materia Auditada, numeral 7, sobre la inexistencia de procedimientos de respaldo de la información, la municipalidad deberá elaborar, formalizar e implementar los manuales que establezcan los parámetros y acciones que permitan la realización de copias de seguridad de la información que manejan los sistemas informáticos, lo que será verificado en la etapa de seguimiento (MC).

10. Sobre lo expuesto en el acápite II, Examen de la Materia Auditada, numeral 8, relativo a las falencias en la sala de servidores, el municipio tendrá que remitir los antecedentes que den cuenta de la implementación de la sala de servidores con su respectiva señalética de seguridad y con las medidas que exige la normativa respectiva, asimismo, deberá acreditar la creación de un registro de acceso y salida a la sala de servidores con el fin de mantener un control de los funcionarios o personal que acceda a ella, lo que será validado en una próxima visita de seguimiento (MC).

11. En relacionado al acápite II, Examen de la Materia Auditada, numeral 9, sobre segregación de funciones en los sistemas computacionales, ese municipio deberá crear, formalizar e implementar medidas y acciones que establezcan la debida segregación de funciones a la cual tienen acceso los distintos funcionarios del municipio, con el fin de disminuir los riesgos en la vulneración de la información que se maneja, lo que será verificado en la etapa de seguimiento (MC).

12. Al tenor de lo expuesto en el acápite II, Examen de la Materia Auditada, numeral 10, relativo a deficiencias relacionadas con las características de las contraseñas, la municipalidad deberá elaborar, formalizar e implementar el reglamento que permita establecer el uso adecuado de las contraseñas de los usuarios y que den cumplimiento a lo señalado en el decreto N° 83, de 2004, Ministerio Secretaría General de la Presidencia.

Adicionalmente, tendrá que mantener un registro de las contraseñas del personal y arbitrar las medidas para que estas cumplan con las exigencias establecidas en la normativa vigente, cuyo avance o término será verificado en la etapa de seguimiento (MC).

13. Sobre lo mencionado en el acápite II, Examen de la Materia Auditada, en cuanto a las casillas electrónicas de los funcionarios, la entidad municipal tendrá que acreditar la regularización respecto del cambio de imagen en los correos electrónicos que se visualizan en el sitio institucional del municipio, lo que será verificado en la etapa de seguimiento (MC).

14. En lo expuesto en el acápite II, Examen de la Materia Auditada, numeral 12, sobre la existencia de un oficial y comité de seguridad, la entidad municipal deberá remitir la creación, designación y formalización del mencionado comité de seguridad, cuyo avance o término será validado en la etapa de seguimiento (MC).

15. Acerca de lo señalado en el acápite II, Examen de la Materia Auditada, numeral 13, sobre los inventarios de hardware y



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

software, el municipio tendrá que remitir la actualización del inventario de activos y documentar la identificación de bienes, lo que será verificado en una futura visita de seguimiento (MC).

16. Sobre lo indicado en el acápite II, Examen de la Materia Auditada, numeral 14, relativo al licenciamiento, disponibilidad y pago del software de la repartición, letras a) y b), el municipio tendrá que acreditar y/o adquirir la utilización de licencias de softwares autorizadas en todos sus equipos computacionales dando cumplimiento a lo señalado en la normativa respectiva de propiedad intelectual.

De igual forma tendrá que arbitrar las medidas para supervisar o vigilar la instalación de softwares no autorizados en los equipos institucionales.

Por último, deberá informar los resultados de las validaciones en los equipos de los funcionarios observados, adjuntando la documentación de respaldo pertinente, aspectos que serán verificados en la etapa de seguimiento (MC).

17. Sobre lo mencionado en el acápite II, Examen de la Materia Auditada, numeral 15, relativo a la existencia de los respaldos, en cuanto a periodicidad, integridad, acceso y un centro de respaldo alternativo, el municipio deberá elaborar, formalizar e implementar los procedimientos que den cuenta de las acciones que se deben realizar para respaldar la información de los sistemas de información, con el fin de resguardar la que se maneja en ellos.

Adicionalmente, le corresponderá acreditar que la documentación e información que manejan los sistemas de información de los servicios traspasados del municipio cuentan con los respaldos respectivos, lo que tendrá que demostrarse en la etapa de seguimiento (MC).

18. En lo relacionado con el acápite II, Examen de la Materia Auditada, numeral 16, sobre incidentes de seguridad detectados en terreno, la municipalidad tendrá que elaborar, formalizar e implementar el procedimiento relativo a la gestión y acceso a la red municipal y además levantar los riesgos de mantener la red municipal en lugares no aptos para ello, cuyo avance o término será validado en la etapa de seguimiento (MC).

19. En cuanto a lo señalado en el acápite II, Examen de la Materia Auditada, numeral 17, sobre pérdida de información en el computador del director del Departamento de Educación, la municipalidad deberá elaborar, formalizar e implementar un procedimiento de desvinculación de funcionarios con asignación de equipos computacionales, con el fin de coordinar con el encargado de informática la revisión y resguardo de la información almacenada en los equipos computacionales, cuyo avance o término será validado en la etapa de seguimiento (MC).

Finalmente, para aquellas observaciones que se mantienen y que fueron categorizadas como MC y LC, la responsabilidad asociada a la validación de las acciones correctivas emprendidas, descritas en el Anexo N°3, será del área encargada del control interno en el municipio, lo que deberá ser acreditado en el Sistema de Seguimiento y Apoyo CGR, que este Organismo



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

Superior de Control puso a disposición de las entidades públicas a contar del 2 de julio de 2018, en conformidad con lo establecido en el oficio N° 14.100, de 2018, de este Órgano Contralor.

Transcríbese al Alcalde, al Secretario Municipal y al Director de Control, todos de la Municipalidad de Bulnes.

Saluda atentamente a Ud.



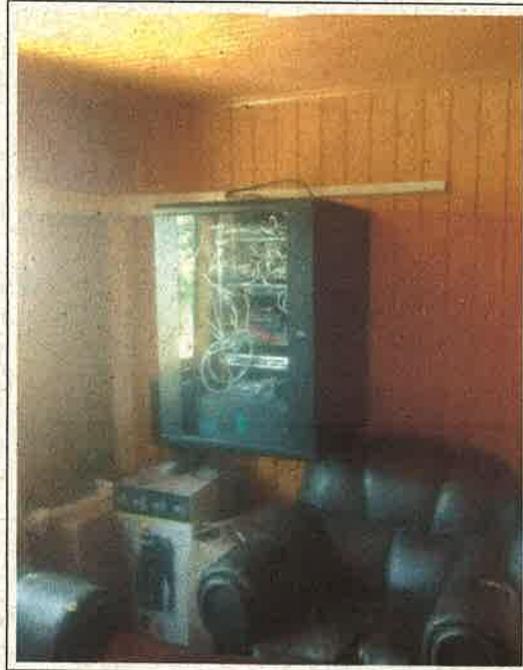
ÁNGELA DOMÍNGUEZ ALBORNOZ
JEFE UNIDAD DE CONTROL EXTERNO
CONTRALORÍA REGIONAL DE ÑUBLE
CONTRALORÍA GENERAL DE LA REPÚBLICA



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

ANEXO N° 1

FOTOGRAFÍAS DISTINTOS SERVIDORES DE LA ENTIDAD MUNICIPAL



Fuente: Fotografía que capta la disposición del RACK del servidor/comunicaciones del DAEM.



Fuente: Fotografía que capta la disposición del RACK de los servidores en la Tesorería Municipal:

PA



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

ANEXO N° 1, CONTINUACIÓN



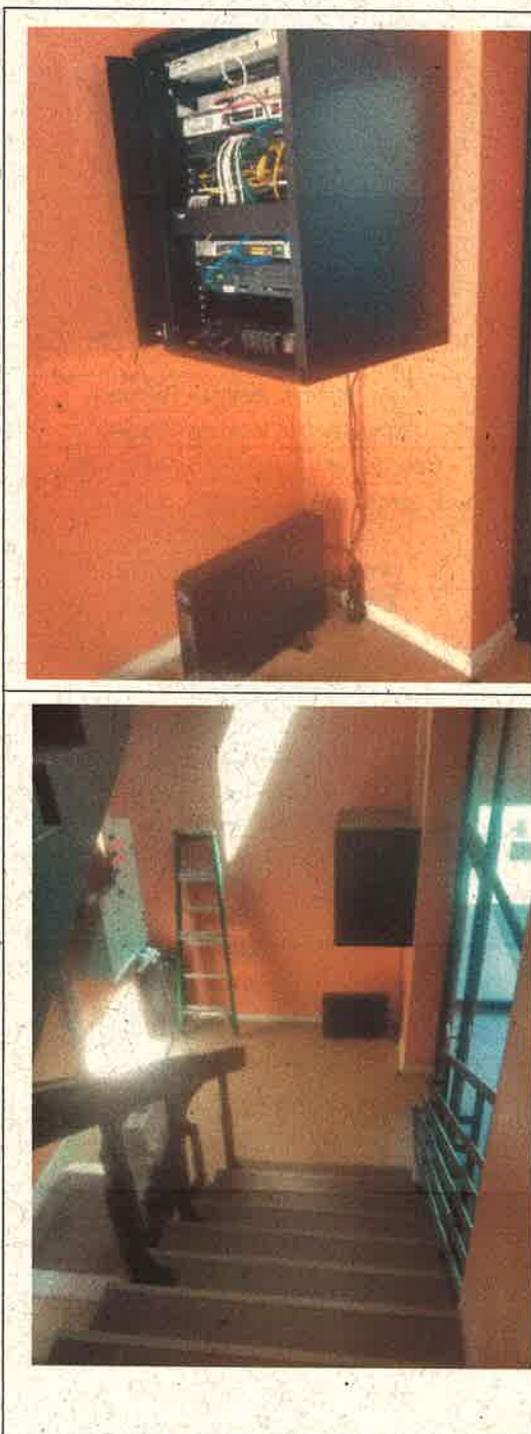
AP

Fuente: Fotografía que capta la disposición del rack de los servidores en la Tesorería Municipal.



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

ANEXO N° 1. CONTINUACIÓN



Fuente: Fotografía que capta la disposición del RACK de comunicaciones de la Municipalidad, en La Casa de la Cultura.



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

ANEXO N° 2

LISTA DE PROGRAMAS UTILIZADOS SIN SUS RESPECTIVAS LICENCIAS

N°	UBICACIÓN	NOMBRE DEL EQUIPO	TIPO DE SOFTWARE
1	Casa de la Cultura.	ENC-Comunicaciones.	Antivirus Avast.
1	Casa de la Cultura.	ENC-Comunicaciones.	PhantomPDF for HP
2	Casa de la Cultura.	GESCULTURA.	Antivirus Avast.
2	Casa de la Cultura.	GESCULTURA.	PhantomPDF for HP
3	Casa de la Cultura	NTBKProyección.	Antivirus Avast.
3	Casa de la Cultura	NTBKProyección.	Winrar.
3	Casa de la Cultura	NTBKProyección.	Office.
4	DAEM, Asistente Social, Becas de Mantención	DESKTOP56ELSDV.	Antivirus Avast.
4	DAEM, Asistente Social, Becas de Mantención	DESKTOP56ELSDV.	Winrar.
5	DAEM.	Convivencia, Bélgica Hidalgo.	Antivirus Avast.
5	DAEM.	Convivencia, Bélgica Hidalgo.	Winrar.
6	DAEM.	Coordinadora JUNAEB, JUNJI PC	Antivirus Avast.
6	DAEM.	Coordinadora JUNAEB, JUNJI PC	Winrar.
7	DAEM.	FAEP, Desktopab5317b.	Antivirus Avast.
7	DAEM.	FAEP, Desktopab5317b.	Winrar JNR.
8	DAEM.	Conciliaciones Bancarias, Finanzassep179.	Antivirus Avast.
8	DAEM.	Conciliaciones Bancarias, Finanzassep179.	Winrar JNR.
9	DAEM.	AlejandroBustam-Finanzas.	Antivirus Avast.
9	DAEM.	AlejandroBustam-Finanzas.	Winrar.
10	DAEM.	Encargada de Finanzas FNZSJDAEM104.	Antivirus Avast.
10	DAEM.	Encargada de Finanzas FNZSJDAEM104.	Winrar.
11	DAEM.	InventarioUTP.	Antivirus Avast.
11	DAEM.	InventarioUTP.	Winrar.
12	DAEM.	Licitaciones-LenovoDAEMPC.	Antivirus Avast.
12	DAEM.	Licitaciones-LenovoDAEMPC.	Winrar.
12	DAEM.	Licitaciones-LenovoDAEMPC.	Microsoft Office Professional Plus 2013.
13	DAEM.	Remuneraciones-Práctica-REMU2DN179.	Antivirus Avast.
13	DAEM.	Remuneraciones-Práctica-REMU2DN179.	Winrar.
14	DAEM, RR.HH.	JefePersonal.	Antivirus Avast.
14	DAEM, RR.HH.	JefePersonal.	Winrar.
14	DAEM, RR.HH.	JefePersonal.	Office 2010.
14	DAEM, RR.HH.	JefePersonal.	PdfComplete
15	DAEM.	UTP2017.	Antivirus Avast.
15	DAEM.	UTP2017.	Winrar.
15	DAEM.	UTP2017.	Cea Ordenadores.

AP



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

Nº	UBICACIÓN	NOMBRE DEL EQUIPO	TIPO DE SOFTWARE
16	Edificio Bianchi, Segundo Piso.	Juzgado Policía Local, MGTRDOJPL144.	Antivirus Avast.
17	Edificio Bianchi, Segundo Piso.	Juzgado Policía Local, SEC2JPL115	Antivirus Avast.
17	Edificio Bianchi, Segundo Piso.	Juzgado Policía Local, SEC2JPL115	Edit Plus Text Editor.
18	Edificio Bianchi, Segundo Piso.	Juzgado Policía Local, SECRE1JPL.	Antivirus Avast.
19	Edificio Bianchi, Segundo Piso.	Tránsito LCONDUCIR40.	Antivirus Avast.
19	Edificio Bianchi, Segundo Piso.	Tránsito LCONDUCIR40.	Winrar.
20	Edificio Bianchi, Segundo Piso.	Tránsito MesonDTT160.	Antivirus Avast.
21	Edificio Bianchi, Segundo Piso.	Tránsito TEST01-RobertoHP.	Antivirus Avast.
22	Edificio Bianchi, Segundo Piso.	Tránsito TEST02-Examen2HP.	Antivirus Avast.
22	Edificio Bianchi, Segundo Piso.	Tránsito TEST02-Examen2HP.	PdfComplete.
23	Edificio Bianchi, Segundo Piso.	Tránsito TEST04-USUARIO4HP.	Antivirus Avast.
23	Edificio Bianchi, Segundo Piso.	Tránsito TEST04-USUARIO4HP.	PdfComplete.
24	Edificio Bianchi.	Tesorería, ApoyoyControl.	Antivirus Avast.
24	Edificio Bianchi.	Tesorería, ApoyoyControl.	Microsoft Office Standard 2016.
25	Edificio Bianchi.	Caja Tesorería16.	Antivirus Avast.
26	Edificio Bianchi.	DControl50.	Antivirus Avast.
27	Edificio Bianchi.	Tesorería SRVBulnes.	Antivirus Avast.
27	Edificio Bianchi.	Tesorería SRVBulnes.	Winrar.
28	Edificio Bianchi.	Tesorería ADM35.	Antivirus Avast.
28	Edificio Bianchi.	Tesorería ADM35.	Winrar.
29	Edificio Bianchi.	Tesorero.	Antivirus Avast.
30	Edificio Bianchi.	Turismo207	Antivirus Avast.
31	EDIFPUB.	Servidor de Aplicaciones CAS.	Antivirus Avast.
31	EDIFPUB.	Servidor de Aplicaciones CAS.	Winrar.
32	Municipio.	Aquisiciones76	Antivirus Avast.
33	Municipio.	Adquisiciones-DESKTOP9B23R5R.	Antivirus Avast.
33	Municipio.	Adquisiciones-DESKTOP9B23R5R.	WinZip.
34	Municipio.	Finanzas-DIRDAF99-JEFE.	Antivirus Avast.
35	Municipio.	Finanzas-FINSZSDAF109.	Antivirus Avast.
36	Municipio Segundo Piso.	Licitaciones-Licitaciones1.	Antivirus Avast.
37	Municipio Segundo Piso.	Obras-Director.	Antivirus Avast.
38	Municipio Segundo Piso.	Obras-Emergencia131-Kimberly.	Antivirus Avast.
39	Municipio Segundo Piso.	Obras-ITODOM104.	Antivirus Avast.
39	Municipio Segundo Piso.	Obras-ITODOM104.	Autodesk.

AF



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

Nº	UBICACIÓN	NOMBRE DEL EQUIPO	TIPO DE SOFTWARE
40	Municipio Segundo Piso.	Obras-Secretaria.	Antivirus Avast.
41	Municipio Segundo Piso.	SECPLAN-LORENA82-Secretaria.	Antivirus Avast.
42	Municipio Segundo Piso.	SECPLAN-SECPLAN191.	Antivirus Avast.
42	Municipio Segundo Piso.	SECPLAN-SECPLAN191.	Autodesk AutoCAD 2018
42	Municipio Segundo Piso.	SECPLAN-SECPLAN191.	Autodesk AutoCAD Civil 3D 2016.
42	Municipio Segundo Piso.	SECPLAN-SECPLAN191.	Autodesk ReCap Pro.
42	Municipio Segundo Piso.	SECPLAN-SECPLAN191.	PdfNitroPro
43	Municipio.	Administradora-Adminmuni113.	Antivirus Avast.
43	Municipio.	Administradora-Adminmuni113.	Winrar.
44	Municipio.	Secretaria Alcalde.	Antivirus Avast.
45	Municipio.	Secretaria Marcela.	Antivirus Avast.
46	Municipio.	Secretaria Municipal-OP-OPPARTES.	Antivirus Avast.
47	Municipio.	Secretaria-SECMUNICIPAL06.	Antivirus Avast.
48	Oficina Transparencia.	43-Bernardita Anavalon	Antivirus Avast.
49	Oficina Transparencia.	45-Johanna Baltierra.	Antivirus Avast.
50	Oficina Transparencia.	46-Carolina Cerda.	Antivirus Avast.
51	Oficina Transparencia.	47-Psicologo.	Antivirus Avast.
51	Oficina Transparencia.	47-Psicologo.	Winrar.
52	Edificio Bianchi.	Tesoreria-Salud-EDDBULNES01.	Antivirus Kaspersky.
53	DAEM.	DESKTOPKU0JQHH-Jefe-Administración.	Antivirus McAfee.
54	DAEM.	RRHH-LAPTOPKH499JQ0.	Antivirus McAfee.
54	DAEM.	RRHH-LAPTOPKH499JQ0.	Winrar.
55	Municipio, Segundo Piso.	Licitciones-Licitaciones1.	Antivirus McAfee.
55	Municipio, Segundo Piso.	Licitciones-Licitaciones1.	Rar Zip Extractor Pro.
56	DAEM.	Convivencia LAPTOP-VF7KSKVE.	Antivirus McAfee.
57	Municipio Segundo Piso.	ARQUITECTOSECPLAN.	Photoshop.
57	Municipio Segundo Piso.	ARQUITECTOSECPLAN.	Autodesk AutoCAD 2019.
57	Municipio Segundo Piso.	ARQUITECTOSECPLAN.	Autodesk ReCap Pro.
57	Municipio Segundo Piso.	ARQUITECTOSECPLAN.	Autodesk Revit 2019.
58	Municipio Segundo Piso.	FORMULADORSECPLAN.	Autodesk AutoCAD 2019.
58	Municipio Segundo Piso.	FORMULADORSECPLAN.	Autodesk ReCap Pro.

AD



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

Nº	UBICACIÓN	NOMBRE DEL EQUIPO	TIPO DE SOFTWARE
58	Municipio Segundo Piso.	FORMULADORSECPLAN.	Autodesk Revit.
58	Municipio Segundo Piso.	FORMULADORSECPLAN.	Autodesk Revit.
59	Casa de la Cultura, Oficina de Comunicaciones.	DESKTOP-32K7S07	Winrar.
60	Casa de la Cultura, Teatro.	NTBKAUDIO.	Winrar.
60	Casa de la Cultura, Teatro.	NTBKAUDIO.	Wondershare Filmora.
60	Casa de la Cultura, Teatro.	NTBKAUDIO.	Splash Pro.
61	DAEM.	Jefe Asistente-PIE2017	Winrar.
61	DAEM.	Jefe Asistente-PIE2017	Winra 5,40 Expired Notification.
62	DAEM, Asistente Social, Vivienda.	Franciscalandd.	Winrar.
63	DAEM.	Coordinadora JUNJI-XIMEUTP	Winrar.
64	DAEM.	Extraescolares-DESKTOPMGG7P47.	Winrar.
65	DAEM.	Mantenimiento-DAEMD456.	Winrar.
65	DAEM.	Mantenimiento-DAEMD456.	Microsoft Office Professional Plus 2013.
66	DAEM.	SVILLABLANCA178.	Winrar.
67	DAEM.	Aminorte-Usuario.	Winrar.
67	DAEM.	Aminorte-Usuario.	Microsoft Office Professional Plus 2010.
68	DAEM.	LAPTOPBK3F9QAD.	Winrar.
68	DAEM.	LAPTOPBK3F9QAD.	Office.
69	Municipio.	Obras-Constructor_Egis.	Winrar.
70	Municipio.	Ajuridico104.	Winrar.
71	Edificio Bianchi, Segundo Piso.	SECJPLME194.	Winzip.
72	DAEM.	RRHHPC.	Microsoft Office Professional Plus 2010.
73	Casa de la Cultura.	Bibliotecario.	PhantomPDF for HP
74	Edificio Bianchi, Segundo Piso.	Tránsito TEST03-Examen3HP	PdfComplete.
74	Edificio Bianchi, Segundo Piso.	Tránsito TEST05-Examen5HP	PdfComplete.
75	DAEM.	InventarioPC.	Winrar.

Fuente: Elaboración propia en base a la información suministrada por el Encargado de Informática de la Municipalidad de Bulnes.



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

ANEXO N° 3

ESTADO DE OBSERVACIONES DEL INFORME FINAL N° 92, DE 2019, MUNICIPALIDAD DE BULNES

N° DE OBSERVACIÓN	MATERIA DE LA OBSERVACIÓN	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN SOLICITADA POR CONTRALORÍA GENERAL EN INFORME FINAL	NIVEL DE COMPLEJIDAD	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DE LA ENTIDAD	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO
Acápito I, numeral 1.	Omisión de un manual de descripción de cargos y funciones para la Unidad de Informática.	Acreditar la confección, formalización e implementación de la unidad de informática y la respectiva descripción del cargo y sus funciones.	MC			
Acápito I, numeral 2.	Inexistencia de auditorías con un enfoque de TI.	Deberá en lo sucesivo incorporar en su plan anual de auditorías revisiones a las políticas, reglamentos e instrucciones relativo a las tecnologías de información.	MC			
Acápito II, numeral 1.	Falta de manuales de procedimientos relacionados con la interoperabilidad entre sistemas institucionales	Acreditar la confección, formalización e implementación del manual de procedimiento sobre interoperabilidad	MC			
Acápito II, numeral 2, letras a), b), c) y d)	Políticas de asignación de cuentas de usuario y claves de acceso.	Demostrar la creación, formalización e implementación del procedimiento relativo a la asignación de cuentas y claves de acceso.	MC			

AP



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

N° DE OBSERVACIÓN	MATERIA DE LA OBSERVACIÓN	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN SOLICITADA POR CONTRALORÍA GENERAL EN INFORME FINAL	NIVEL DE COMPLEJIDAD	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DE LA ENTIDAD	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO
Acápito II, numeral 3.	Existencia y utilización de políticas, planes o procedimientos formalizados sobre uso, almacenamiento, acceso y distribución de mensajes electrónicos.	Informar sobre la creación, formalización e implementación, del reglamento que permita el correcto uso del correo electrónico y de servicios de internet.	MC			
Acápito II, numeral 4.	Ausencia de un plan de contingencia municipal.	Demostrar la elaboración, formalización e implementación del plan de contingencia que asegure la continuidad de las operaciones críticas.	MC			
Acápito II, numeral 5.	Procedimientos para resguardar la confidencialidad de la información.	Acreditar la elaboración, formalización e implementación del procedimiento sobre el resguardo en la confidencialidad de la información.	MC			
Acápito II, numeral 6.	Política de seguridad de la información.	Acreditar la creación, formalización e implementación de las políticas de seguridad de la información.	MC			
Acápito II, numeral 7.	Inexistencia de procedimientos de respaldo de la información.	Informar sobre la creación, formalización e implementación de los manuales sobre las copias y respaldo de seguridad.	MC			
Acápito II, numeral 8.	Falencia en la sala de servidores.	Informar sobre la implementación de la sala de servidores y su respectiva señalética de seguridad e implementación de un registro de entrada y salida de las dependencias de los servidores.	MC			
Acápito II, numeral 9.	Segregación de funciones en los sistemas computacionales.	Crear, formalizar e implementar medidas y acciones que establezcan la debida segregación de funciones a la cual tienen acceso los distintos funcionarios del municipio.	MC			



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

N° DE OBSERVACIÓN	MATERIA DE LA OBSERVACIÓN	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN SOLICITADA POR CONTRALORÍA GENERAL EN INFORME FINAL	NIVEL DE COMPLEJIDAD	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DE LA ENTIDAD	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO
Acápito II, numeral 10.	Deficiencias relacionadas con las características de las contraseñas.	<p>Acreditar la confección, formalización e implementación del reglamento sobre uso de contraseñas dando cumplimiento con lo señalado en el decreto N° 83, de 2004, Ministerio Secretaría General de la Presidencia.</p> <p>Proporcionar un registro de las contraseñas del personal y arbitrar las medidas para que estas cumplan con las exigencias establecidas en la normativa vigente.</p>	MC			
Acápito II, numeral 11.	Casillas electrónicas de los funcionarios.	Informar sobre la regularización respecto del cambio de imagen de los correos electrónicos institucionales publicados en el sitio web del municipio.	MC			
Acápito II, numeral 12.	Existencia de un oficial y comité de seguridad.	Remitir la creación, designación y formalización del mencionado comité de seguridad.	MC			
Acápito II, numeral 13.	Inventarios de hardware y software.	Mostrar la actualización del inventario de activos y documentar la identificación de bienes computacionales.	MC			
Acápito II, numeral 14.	Licenciamiento, disponibilidad y pago del software de la repartición, letras a) y b).	<p>Acreditar la adquisición y utilización de licencias en los equipos computacionales.</p> <p>Mostrar las medidas para supervisar o vigilar la instalación de softwares no autorizados en los equipos institucionales.</p> <p>Informar los resultados de las validaciones en los equipos de los funcionarios observados, adjuntando la documentación de respaldo pertinente.</p>	MC			

AP



CONTRALORÍA GENERAL DE LA REPÚBLICA
CONTRALORÍA REGIONAL DE ÑUBLE
UNIDAD DE CONTROL EXTERNO

N° DE OBSERVACIÓN	MATERIA DE LA OBSERVACIÓN	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN SOLICITADA POR CONTRALORÍA GENERAL EN INFORME FINAL	NIVEL DE COMPLEJIDAD	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DE LA ENTIDAD	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO
Acápito II, numeral 15.	Existencia de los respaldos en cuanto a la periodicidad, integridad, acceso y un centro de respaldo alternativo.	Informar sobre la elaboración, formalización e implementación de los manuales y procedimientos en cuanto a los respaldos de seguridad que deben mantener el municipio.	MC			
Acápito II, numeral 16.	Incidentes de seguridad detectados en terreno.	Elaborar, formalizar e implementar el procedimiento relativo a incidentes de seguridad y de acceso a la red municipal.	MC			
Acápito II, numeral 17.	Sobre pérdida de información en el computador del director del DAEM.	Acreditar la confección, formalización e implementación de un procedimiento sobre desvinculación de funcionarios con asignación de equipos computacionales.	MC			

AP