POR EL CUIDADO Y BUEN USO
DE LOS RECURSOS PÚBLICOS

CONTRALORÍA REGIONAL DE ATACAMA
UNIDAD DE CONTROL EXTERNO

INFORME FINAL

MUNICIPALIDAD DEDIEGO DE ALMAGRO

INFORME N° 1.022 / 2021
25 DE ABRIL DE 2022

OBJETIVOS DE DESARROLLO SOSTENIBLE

CONTRALORÍA GENERAL DE LA REPÚBLICA
CHILE

POR EL CUIDADO Y BUEN USO
DE LOS RECURSOS PÚBLICOS

Remite Informe Final N° 1022, de 2021

Escritorio CGR - Comunicación de Informe Final de Observaciones de auditoría simplificada <notificaciones.sicaescritorio@cgr.cl>

Lun 25-04-2022 17:41

Para: [redacted]

2 archivos adjuntos (1 MB)

FIRMADO_INFORME FINAL 1.022-21 MUNICIPALIDAD DE DIEGO DE ALMAGRO.pdf; Oficio_E2070722022.pdf;

Señor(a) [redacted]

Junto con saludar y de acuerdo con lo establecido en el artículo 25 de la resolución N° 10, de 2021, que Fija Normas que Regulan las Auditorías efectuadas por la Contraloría General de la República, se remite a Ud., para su conocimiento y fines pertinentes el Informe Final N° 1022, de 2021, que contiene el resultado de la auditoría que se practicara en MUNICIPALIDAD DE DIEGO DE ALMAGRO.

Saludos cordiales.

Nota: No responder este mensaje.

CONTRALORÍA GENERAL DE LA REPÚBLICA
Teatinos 56, Santiago, Chile
www.contraloria.cl

Remite Informe Final N° 1022, de 2021

Escritorio CGR - Comunicación de Informe Final de Observaciones de auditoría simplificada <notificaciones.sicaescritorio@cgr.cl>

Lun 25-04-2022 17:41

Para: [redacted]

Señor(a) [redacted]

Junto con saludar y de acuerdo con lo establecido en el artículo 25 de la resolución N° 10, de 2021, que Fija Normas que Regulan las Auditorías efectuadas por la Contraloría General de la República, se remite a Ud., para su conocimiento y fines pertinentes el Informe Final Nº 1022, de 2021, que contiene el resultado de la auditoría que se practicara en MUNICIPALIDAD DE DIEGO DE ALMAGRO.

Saludos cordiales.

Nota: No responder este mensaje.

CONTRALORÍA GENERAL DE LA REPÚBLICA
Teatinos 56, Santiago, Chile
www.contraloria.cl

Remite Informe Final N° 1022, de 2021

Escritorio CGR - Comunicación de Informe Final de Observaciones de auditoría simplificada <notificaciones.sicaescritorio@cgr.cl>

Lun 25-04-2022 17:41

Para: [redacted]

Señor(a) [redacted]

Junto con saludar y de acuerdo con lo establecido en el artículo 25 de la resolución N° 10, de 2021, que Fija Normas que Regulan las Auditorías efectuadas por la Contraloría General de la República, se remite a Ud., para su conocimiento y fines pertinentes el Informe Final Nº 1022, de 2021, que contiene el resultado de la auditoría que se practicara en MUNICIPALIDAD DE DIEGO DE ALMAGRO.

Saludos cordiales.

Nota: No responder este mensaje.

CONTRALORÍA GENERAL DE LA REPÚBLICA
Teatinos 56, Santiago, Chile
www.contraloria.cl

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

REF. N°: 30.596/2022
30.614/2022
PREG N°: 3.045/2021
UCE. N°: 254

REMITE INFORME FINAL DE AUDITORÍA QUE INDICA.

COPIAPÓ, 25 de abril de 2022

Se remite, para su conocimiento y fines pertinentes, el Informe Final N° 1.022, de 2021, sobre Seguridad de los Sistemas de Información de la Municipalidad de Diego de Almagro.

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.

Finalmente, cabe recordar que los datos personales, información personal y datos sensibles contenidos en el Informe Final que se remite, se encuentran protegidos conforme a la ley N° 19.628, sobre Protección de la Vida Privada, y a cuyo respecto se deberán adoptar las medidas pertinentes a fin de asegurar su protección y uso adecuado, conforme a las disposiciones del referido cuerpo normativo.

Saluda atentamente a Ud.,

AL SEÑOR
ALCALDE
MUNICIPALIDAD DE DIEGO DE ALMAGRO
PRESENTE

DISTRIBUCIÓN:

- Unidad de Control Externo de la Contraloría Regional de Atacama
- Unidad de Apoyo al Cumplimiento de la Contraloría Regional de Atacama

Firmado electrónicamente por:	
Nombre	EDUARDO VELIZ GUAJARDO
Cargo	Contralor Regional
Fecha firma	25/04/2022
Código validación	bbrWeNREv
URL validación	https://www.contraloria.cl/validardocumentos

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

REF. N°: 30.596/2022
30.614/2022
PREG N°: 3.045/2021
UCE. N°: 255

REMITE INFORME FINAL DE AUDITORÍA QUE INDICA.

COPIAPÓ, 25 de abril de 2022

Se remite, para su conocimiento y fines pertinentes, el Informe Final N° 1.022, de 2021, sobre Seguridad de los Sistemas de Información de la Municipalidad de Diego de Almagro.

Cabe recordar que los datos personales, información personal y datos sensibles contenidos en el Informe Final que se remite, se encuentran protegidos conforme a la ley N° 19.628, sobre Protección de la Vida Privada, y a cuyo respecto se deberán arbitrar las medidas pertinentes a fin de asegurar su protección y uso adecuado, conforme a las disposiciones del referido cuerpo normativo.

Saluda atentamente a Ud.,

AL SEÑOR
DIRECTOR DE CONTROL
MUNICIPALIDAD DE DIEGO DE ALMAGRO
PRESENTE

DISTRIBUCIÓN:

- Unidad de Control Externo de la Contraloría Regional de Atacama

Firmado electrónicamente por:	
Nombre	EDUARDO VELIZ GUAJARDO
Cargo	Contralor Regional
Fecha firma	25/04/2022
Código validación	bbrWeNRrC
URL validación	https://www.contraloria.cl/validardocumentos

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

REF. N°: 30.596/2022
30.614/2022
PREG N°: 3.045/2021
UCE. N°: 256

REMITE INFORME FINAL DE AUDITORÍA QUE INDICA.

COPIAPÓ, 25 de abril de 2022

Se remite, para su conocimiento y fines pertinentes, el Informe Final N° 1.022, de 2021, sobre Seguridad de los Sistemas de Información de la Municipalidad de Diego de Almagro, 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 entregándole copia del mismo.

Al respecto, Ud. deberá acreditar ante esta Contraloría General, en su calidad de secretaria 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.,

AL SEÑOR
SECRETARIO MUNICIPAL
MUNICIPALIDAD DE DIEGO DE ALMAGRO
PRESENTE

DISTRIBUCIÓN:

- Unidad de Control Externo de la Contraloría Regional de Atacama

Firmado electrónicamente por:	
Nombre	EDUARDO VELIZ GUAJARDO
Cargo	Contralor Regional
Fecha firma	25/04/2022
Código validación	bbrWeNSJk
URL validación	https://www.contraloria.cl/validardocumentos

INDICE

GLOSARIO

TÉRMINO	CONCEPTO
NMAP[1]	Del inglés "Network Mapper", es una utilidad de licencia gratuita y de código abierto para la investigación de redes y la auditoría de seguridad.
Firewall[2]	Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet. Un firewall puede ser hardware, software o ambos.
Log Shipping[3]	Proceso de respaldar automáticamente la base de datos y el log de transacciones, restaurándolos en un servidor de respaldo. Esto mantiene a los dos equipos en sincronía en caso de que el servidor de producción tenga alguna falla.
Downgrade[4]	Acción de instalar una versión anterior de cualquier software.
Logs[5]	Son archivos de texto normales, estos ficheros registran todos los procesos que han sido definidos como relevantes por el programador de la aplicación, en caso de que un fallo del sistema elimine información de la base de datos, el log será la clave para la restauración completa de la base de datos correspondiente.

[1] Sitio web Nmap. Org., https://nmap.org/book/man.html#man-description
[2] Sitio web de CISCO, https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html
[3] Sitio web Microsoft, https://docs.microsoft.com/en-us/sql/database-engine/log-shipping/about-log-shipping-sql-server?view=sql-server-ver15
[4] Sitio web Dell Technologies, https://www.dell.com/support/kbdoc/es-cl/000138362/una-comprensi%C3%B3n-de-los-derechos-de-cambio-a-una-versi%C3%B3n-anterior-y-los-derechos-de-cambio-a-una-versi%C3%B3n-anterior-de-microsoft-windows-8-8-8-1-y-10?lang=es
[5] Sitio web Digital Guide IONOS, https://www.ionos.es/digitalguide/online-marketing/analisis-web/el-log-el-archivo-de-registro-de-procesos-informaticos/#:~:text=Los%20logs%20son%20archivos%20de,el%20programador%20de%20la%20aplicaci%C3%B3n.

RESUMEN EJECUTIVO
Informe Final N° 1.022, de 2021,
Municipalidad de Diego de Almagro

Objetivo: Efectuar una auditoría al Macroproceso de Tecnologías de la Información, con la finalidad de revisar y evaluar el nivel de seguridad informática implementado por esa entidad, a través de la existencia y aplicación de políticas, normas y procedimientos de seguridad informática que permitan asegurar la integridad, confiabilidad y confidencialidad de la información en sus sistemas informáticos y redes de comunicación, conforme a las Normas Técnicas aplicables para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos, aprobada por el artículo primero del decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia.

Preguntas de Auditoría:

- ¿La entidad ha implementado controles para la gestión de la seguridad de la información?

Principales resultados:

- Se verificó que si bien, la Municipalidad de Diego de Almagro cuenta con un manual de procedimientos de informática y un manual de procedimiento para el alta, baja y cambio de usuarios que trabajan con los Sistemas de Información Financiera Municipal, SIFIM y Mercado Público, estos documentos datan del año 2012 y se encuentran desactualizados, sin formalizar y no han sido sometidos a procesos de revisión, vulnerando el numeral 1 del capítulo I, de la resolución exenta N° 1.485, de 1996, que indica que el director de toda institución pública debe asegurar no sólo el establecimiento de una estructura de control interno adecuada, sino también la revisión y actualización de esta para mantener su eficacia, por lo que el servicio deberá remitir estos manuales debidamente actualizados y formalizados, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

- Se constató que el municipio no posee un inventario de activos de tecnologías de información, que registre tanto el equipamiento físico (computadores y periféricos), como el software adquirido y existente, y que se encuentren individualizados mediante códigos de inventario asignados por la institución, lo que impide la adecuada revisión, control e identificación inmediata de este tipo de bienes. La situación no se condice con la resolución exenta N° 1.485, de 1996, lo que constituye una debilidad de control interno, por lo cual el servicio deberá remitir el inventario de los activos computacionales -hardware y software-, debidamente registrados con códigos de inventario asignados por la institución, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

- Se constató que el municipio no ha designado formalmente a un funcionario que cumpla las labores como Encargado de Seguridad de la Información, lo

que imposibilita el desarrollo de políticas de seguridad, asesoramiento a los departamentos que conforman la entidad comunal y que requieran de procedimientos tecnológicos, coordinación de respuesta ante incidentes que afecten a los activos de información, entre otras funciones. Asimismo, Se verificó que no existe un Comité de Seguridad de la Información, lo que impide emitir lineamientos para la gestión de la seguridad de la información; revisar y aprobar las políticas de seguridad; revisar y analizar incidentes de seguridad, entre otras actividades, incumpliendo los artículos 12 y 37, respectivamente del decreto N° 83 , de 2004, sobre Seguridad Organizacional, por lo cual el servicio deberá remitir su designación formal, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

- Se constató que la entidad edilicia no ha efectuado una evaluación de los riesgos de seguridad, vulnerando lo establecido en el numeral 0.4, de la NCh ISO 27.002, de 2009, la que señala que los requisitos de seguridad se identifican mediante una evaluación metódica de los riesgos. El gasto en controles se debería equilibrar con el perjuicio en el negocio, resultante de los fallos de seguridad, por lo cual la Municipalidad, deberá remitir el informe de evaluación de riesgos, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

- Se evidenció que en el año 2017, y en los meses de marzo y abril de 2021, el servicio fue afectado por el virus ramsonware de extensión .OPTIMUS y .EKING, comprometiendo la información de todas las bases de datos administradas por el municipio de las áreas municipal, salud y educación, desde los sistemas giradores hasta los sistemas financiero-contables proporcionados por CAS Chile e incluidos en el proyecto SIFIM.

- Se verificó que la infraestructura tecnológica de seguridad informática implementada por el municipio, no se condice con los eventos provocados por la acción de software malicioso de mayor grado de peligrosidad y que afectó la integridad de sus servicios, toda vez que el software antivirus corresponde a la versión que viene instalado por defecto en el sistema operativo Windows y en algunos equipos se ha instalado un antivirus de libre edición, los cuales resultan ser ineficaces para brindar protección a sus sistemas, incumpliendo el artículo 26, letra a) del decreto N° 83, de 2004, por lo que el ente edilicio, deberá remitir un informe sobre la habilitación del equipo firewall que indica adquirir, además de un plan de mejora a su infraestructura tecnológica que incluya la adquisición de un software antivirus, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

- La entidad no proporcionó a este organismo fiscalizador los contratos y/o convenios sobre servicios externalizados, específicamente el contrato actual de SIFIM, por tanto, no fue posible tomar conocimiento de las responsabilidades que deben ser atribuidas al municipio o a la empresa GTD

sobre los procesos de copias de seguridad y restauración de sus sistemas, sobre todo tomando en cuenta los eventos de pérdida de información a causa del virus que afectó la entidad municipal, por lo que la entidad, deberá remitir el convenio actual de SIFIM y una aclaración de las responsabilidades que deben ser atribuidas al municipio o a la empresa GTD sobre los procesos de copias de seguridad y restauración de sus sistemas, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

- Sobre Licenciamiento de software, es menester indicar que a través del decreto de pago N° 891, de fecha 6 de mayo de 2016, el municipio pagó al proveedor Magens S.A. un total de $39.442.984 por la adquisición de 145 licencias Microsoft Office Standard 2016, 12 licencias Microsoft Windows Professional 10, 55 licencias SQLCAL 2014 y 55 licencias Windows Server Cal 2012.

- En relación a las 145 licencias perpetuas de Office Standard 2016 OPL NL Gov, adquiridas por la Municipalidad de Diego de Almagro, a través del citado decreto de pago N° 891, se advirtió, que, dichas licencias no se encontraban instaladas, toda vez que en los equipos informáticos mantienen una versión de software distinto al adquirido. Si bien la entidad explicó que es posible instalar una versión anterior (downgrade), se observa una vulneración a los principios de responsabilidad, eficiencia, eficacia, contenidos en los artículos 3° y 11 de la referida ley N° 18.575, toda vez que, la entidad comunal incurrió en pagos por concepto de software que no utilizó, pues conforme a los documentos de pago, la adquisición original correspondía a la versión 2016, última versión disponible en el año descrito, lo cual se da cuenta en el valor del producto, por lo cual el servicio deberá remitir, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, un plan de renovación de equipos computacionales que permitan la instalación del software adquirido, que incluya responsables y plazos concretos para su ejecución. Además, ese Municipio deberá, en lo sucesivo, efectuar un análisis previo para establecer las compatibilidades necesarias entre su plataforma de hardware y software, a fin de evitar situaciones como las descritas y dar cumplimiento a los principios de eficiencia y eficacia que rigen a los Órganos de la Administración del Estado.

- Cabe destacar que, esta Contraloría observó debilidades de seguridad en la sala de servidores como la Inexistencia de puerta de cortafuego, Inexistencia de sistemas de emergencia, Falta de sistema de iluminación de emergencia, Instalaciones eléctricas, equipo de ventilación sin funcionar, ausencia de bitácoras, entre otros, los cuales vulneran la normativa descrita en la Norma Chile ISO 27.001 de 2009 y el Decreto N° 83 de 2004, por lo que la Municipalidad de Diego de Almagro, deberá remitir un plan de mejora para la sala de servidores que incluya la instalación, mejora o modificación de los elementos observados, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

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

PREG N° 3.045/2021
REFs. N^{os}. 30.596/2022
30.614/2022

INFORME FINAL DE AUDITORÍA N° 1.022 DE 2021, SOBRE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA MUNICIPALIDAD DE DIEGO DE ALMAGRO.

_____

COPIAPÓ, 25 de abril de 2022

En cumplimiento del plan anual de fiscalización de esta Contraloría Regional para el año 2021, y en conformidad con lo establecido en la ley N° 10.336, de Organización y Atribuciones de la Contraloría General de la República, se efectuó una auditoría a los sistemas de información mantenidos en la Municipalidad de Diego de Almagro, con la finalidad de revisar y evaluar el nivel de seguridad informática implementado por la entidad, por el período comprendido entre el 6 de julio al 11 de octubre de 2021.

JUSTIFICACIÓN

A partir de la ejecución de las auditorías de sistemas desarrolladas por esta Contraloría Regional de la República, se han advertido deficiencias en los sistemas informáticos mantenidos por los servicios públicos de la Administración del Estado, que afectan la seguridad y confiabilidad de estos. Además, se consideró que durante los últimos años se han conocido públicamente ataques que han afectado el normal funcionamiento de estos sistemas, por lo que resulta relevante evaluar el nivel de seguridad implementado por las entidades.

Asimismo, a través de la presente auditoría esta Contraloría General 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.

En tal sentido, esta revisión se enmarca en el ODS, N° 16, Paz, Justicia e Instituciones Sólidas, específicamente, con la meta N° 16.6, Crear a todos los niveles instituciones eficaces y transparentes que rindan cuentas.

AL SEÑOR
EDUARDO VELIZ GUAJARDO
CONTRALOR REGIONAL DE ATACAMA
CONTRALORÍA GENERAL DE LA REPÚBLICA
PRESENTE

ANTECEDENTES GENERALES

La Municipalidad de Diego de Almagro, es una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio, cuya misión según lo establece el artículo 1° de la ley N° 18.695, Orgánica Constitucional de Municipalidades, es satisfacer las necesidades de la comunidad local y asegurar su participación en el progreso económico, social y cultural de la comuna.

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 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, cabe recordar que la seguridad de la información utilizada por los órganos de la Administración del Estado en términos de confidencialidad y disponibilidad se debe sujetar a lo establecido en el decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, el que 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.

Enseguida, es preciso señalar que a través de la resolución exenta N° 1.535, de 2009, del entonces Ministerio de Economía, Fomento y Reconstrucción, se declaró como norma oficial de la República de Chile, entre otras, la Norma Chilena ISO 27.002, de 2009, sobre Tecnología de la información - Código de prácticas para la gestión de la seguridad de la información, y reemplaza a la Norma Chilena 2.777, de 2003, como complementaria para efectos de lo establecido en el citado decreto N° 83, de 2004.

Asimismo, se debe tener presente lo establecido en la ley N° 20.285, sobre Acceso a la Información Pública, ley N° 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma y ley N° 17.336, de Propiedad Intelectual.

Enseguida, es oportuno señalar que la citada entidad cuenta con un funcionario especialista en informática, desempeñándose como jefe del área, desde el 2 de enero de 2020, según consta en el decreto alcaldicio N° 144 de 2020, cuya dependencia recae en la Secretaría Municipal de la Entidad.

Por medio del oficio N° E180176, de 28 de enero de 2022, de esta procedencia, con carácter confidencial, fue puesto en conocimiento de la Municipalidad de Diego de Almagro, el preinforme de auditoria N° 1.022, de 2021, con la finalidad de que formularan los alcances y precisiones que a su juicio procedieran, lo que se concretó por medio de los ordinarios N^{os} 128 y 144,

ingresados a esta Contraloría General el 1 y 2 de marzo de esa misma anualidad, respectivamente.

OBJETIVO

Efectuar una auditoría al macroproceso de Tecnologías de Información, con la finalidad de revisar y evaluar el nivel de seguridad informática implementado en la Municipalidad de Diego de Almagro, a través de la existencia y aplicación de políticas, normas y procedimientos de seguridad informática que permitan verificar la integridad, confiabilidad y confidencialidad de la información en sus sistemas informáticos, y redes de comunicación, conforme a las Normas Técnicas aplicables a los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos, aprobada por el artículo primero del decreto N° 83, de 2004, del Ministerio de Secretaría General de la Presidencia.

No obstante, es menester hacer presente que esta auditoría se ejecutó durante la vigencia del estado de excepción constitucional de catástrofe, por calamidad pública, en el territorio de Chile, declarado a través del decreto supremo N° 104, de 2020, del Ministerio del Interior y Seguridad Pública, por un periodo de 90 días a contar del día 18 de marzo de 2020, medida que ha sido prorrogada por los decretos supremos N^{os} 269, 400 y 646, todos de 2020, y 72, de 2021, de esa misma cartera ministerial, cuyas circunstancias afectaron el normal desarrollo de esta fiscalización, en lo que dice relación con la revisión del total de la muestra, limitando a su vez la posibilidad de efectuar validaciones en terreno.

METODOLOGÍA

El examen se practicó de acuerdo con la metodología de auditoría de este Organismo Superior de Control, y de las disposiciones contenidas en la resolución N° 10, de 2021, que Establece Normas que Regulan las Auditorías Efectuadas por la Contraloría General de la República y deja sin efecto la resolución N° 20, de 2015, de este origen, además de los procedimientos de control aprobados mediante resolución exenta N° 1.485, de 1996, que Aprueba Normas de Control Interno de la Contraloría General, considerando los resultados de la evaluación de control interno y determinándose la realización de pruebas de auditoría en la medida que se estimaron necesarias.

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 entiende por Altamente complejas (AC)/Complejas (C), aquellas observaciones que, de acuerdo con su magnitud, reiteración, detrimento patrimonial, graves debilidades de control interno, 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.

UNIVERSO Y MUESTRA

De acuerdo con los antecedentes proporcionados por la entidad fiscalizada, durante el periodo examinado, la cantidad de equipos informáticos asciende a un total de 80 registros.

Las partidas sujetas a examen se determinaron mediante un muestreo analítico, considerando aquellos equipos que fueron informados por la Municipalidad de Diego de Almagro y que manejan los sistemas de gestión, cuya muestra asciende a 20 equipos computacionales, lo que equivale al 25% del universo antes identificado.

RESULTADO DE LA AUDITORÍA

El resultado de la auditoría practicada se expone a continuación:

I. ASPECTOS DE CONTROL INTERNO

Como cuestión previa, es útil indicar que el control interno es un proceso integral y dinámico que se adapta constantemente a los cambios que enfrenta la organización, es efectuado por la alta administración y los funcionarios de la entidad, está diseñado para enfrentar los riesgos y para dar una seguridad razonable del logro de la misión y objetivos de la entidad; cumplir con las leyes y regulaciones vigentes; entregar protección a los recursos de la entidad contra pérdidas por mal uso, abuso, mala administración, errores, fraude e irregularidades, así como también, para la información y documentación, que también corren el riesgo de ser mal utilizados o destruidos.

En este contexto, el estudio de la estructura de control interno de la entidad y de sus factores de riesgo, permitió obtener una comprensión del entorno en que se ejecutan las operaciones relacionadas con la materia auditada, del cual se desprenden las siguientes observaciones:

1. Debilidades generales de control interno.

1.1 Sobre manuales de procedimientos sin formalizar.

Se verificó que si bien, la Municipalidad de Diego de Almagro cuenta con un manual de procedimientos de informática, el cual fue aprobado por el Concejo Municipal, según consta en acta de acuerdo de concejo N° 100, de fecha 22 de mayo de 2012, este documento no se encuentra debidamente formalizado por la autoridad comunal.

La situación planteada vulnera lo contenido en el artículo 3° de la ley N° 19.880, que Establece Bases de los Procedimientos que Rigen los Actos de los Órganos de la Administración del Estado, en donde señala que las decisiones escritas que adopte la Administración se expresarán por medio de actos administrativos.

Asimismo, la mencionada normativa señala, que para estos efectos, se entenderá por acto administrativo, las decisiones formales que emitan los Órganos de la Administración del Estado en las cuales contienen declaraciones de voluntad, realizadas en el ejercicio de la administración pública.

Cabe agregar, que según lo prescribe el artículo 12, inciso cuarto, de la ley N° 18.695, ya señalada, tales actos administrativos se denominan decretos alcaldicios cuando se trata de resoluciones emanadas de los alcaldes que versan sobre casos particulares.

En su respuesta, la entidad adjuntó el memorándum N° 54, de fecha 28 de febrero de 2022, mediante el cual, don [redacted], alcalde (s) instruyó a don [redacted], Director de Control Interno, decretar el Manual de Procedimiento de Informática, aprobado con fecha 22 de mayo del año 2012. Además, indica que, se procederá a formar un equipo de trabajo que permita realizar el proceso de revisión y/o actualización del documento indicado.

Referente a este punto, se mantiene lo observado, dado que las medidas anunciadas por el servicio, corresponden a acciones futuras no materializadas a la fecha, por lo cual ese municipio deberá, remitir el manual de procedimientos de informática, debidamente formalizado, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe.

1.2 Manual de procedimiento desactualizado.

En cuanto al manual de procedimiento para el alta, baja y cambio de usuarios que trabajan con los Sistemas de Información Financiera Municipal, SIFIM, y Mercado Público, autorizado mediante acta de acuerdo N° 79, del Concejo Municipal, de fecha 8 de mayo de 2012 y el manual de procedimientos de informática, aprobado a través del acuerdo N° 100 del Concejo Municipal, de fecha 23 de mayo de esa misma anualidad, se constató que tales documentos no han sido sometidos a procesos de revisión y/o actualización desde esa fecha.

Al respecto, es útil recordar que el numeral 1 del capítulo I, de la referida resolución exenta N° 1.485, de 1996, indica que el director de toda institución pública debe asegurar no sólo el establecimiento de una estructura de control interno adecuada, sino también la revisión y actualización de ésta para mantener su eficacia.

Luego, el numeral 45 dispone que la documentación relativa a las estructuras de control interno debe incluir datos sobre la estructura y políticas de la institución, sobre sus categorías operativas, objetivos y procedimientos de control. Esta información debe figurar en documentos tales como la guía de gestión, las políticas administrativas y los manuales de operación y de contabilidad.

En su respuesta, la autoridad comunal señaló que estos manuales han sido revisados y actualizados de forma interna en

la medida de lo necesario, pero no se han sometido nuevamente al concejo para su aprobación, por lo que revisarán dentro de una comisión y se actualizarán para adecuarse a los cambios tecnológicos actuales y conforme a las normativas legales vigentes.

Referente a este punto, se mantienen las observaciones, debido a que las gestiones anunciadas, no se han materializado, por lo cual la entidad deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir los documentos debidamente actualizados y formalizados para su validación.

1.3 Falta de cumplimiento a las disposiciones contenidas en manuales de procedimientos.

Sobre el particular, es menester indicar que si bien, el municipio cuenta con un manual de procedimiento que entrega orientaciones e instrucciones sobre el accionar de los usuarios de las estaciones de trabajo, que reglamenta el uso, manejo, distribución, modificación y manipulación de los elementos informáticos, se constató que la entidad edilicia no dio cumplimiento a las disposiciones contenidas en dicho instrumento, las que se individualizan en el anexo N° 1, lo que originó situaciones como las descritas en el Acápite II Examen de la Materia Auditada, en los numerales 4.c), 4.d), 7.b), 7.f), 9.i), 9.j), 11, 13.d) del presente informe.

Lo expuesto anteriormente, no se condice con lo establecido en el numeral 38 y 39 de la referida resolución exenta N° 1.485, de 1996, que dispone que los directivos deben vigilar continuamente sus operaciones y adoptar inmediatamente las medidas oportunas ante cualquier evidencia de irregularidades o de actuación contraria a los principios de economía, eficiencia y eficacia y 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.

En su respuesta, la entidad municipal señaló que se deberá hacer énfasis y distribuir nuevamente en todas las direcciones municipales los manuales de procedimientos informáticos a fin de evitar incurrir en faltas que afecten al servicio.

Según lo anterior, se debe mantener lo observado, dado que las medidas comprometidas por el servicio corresponden a hechos futuros, por lo cual la entidad, deberá en un plazo no superior a 60 días hábiles contados desde la recepción del presente informe, emitir un informe con las gestiones realizadas tendientes a subsanar las observaciones descritas en el Anexo N°1, adjuntando respaldo de las difusiones al personal a través de correos electrónicos, registro de capacitaciones y actas de entrega de documentación, además de abordar las responsabilidades que le competen al Departamento de Informática sobre la materia observada.

2. Situaciones de riesgo no controlados por el servicio.

2.1 Ausencia de un inventario de activos de tecnologías de la información.

Se constató que el municipio no posee un inventario de activos de tecnologías de información, que registre tanto el equipamiento físico (computadores, impresoras, teclados, mouses, cargadores de notebook u otros), como el software adquirido y existente, y que se encuentren individualizados mediante códigos de inventario asignados por la institución, lo que impide la adecuada revisión, control e identificación inmediata de este tipo de bienes.

Al respecto, cabe hacer presente que la falta de inventario no permite mitigar el riesgo del mal uso de los dispositivos, controlar su vida útil y su deterioro o que sean sustraídos desde las dependencias de la entidad comunal.

La situación planteada no se condice con los expuesto en los numerales 44 y 46 de la citada resolución exenta N° 1.485, de 1996, los que indican que, una institución debe tener pruebas escritas (1) de su estructura de control interno, incluyendo sus objetivos y procedimientos de control, y (2) 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 y que la documentación sobre transacciones y hechos significativos debe ser completa y exacta y facilitar el seguimiento de la transacción o hecho (y de la información concerniente) antes, durante y después de su realización.

Finalmente, expone el numeral 47 que, la documentación de las estructuras de control interno, de las transacciones y de hechos importantes debe tener un propósito claro, ser apropiada para alcanzar los objetivos de la institución y servir a los directivos para controlar sus operaciones y a los fiscalizadores u otras personas para analizar dichas operaciones. Toda documentación que no tenga una meta clara corre el riesgo de diezmar la eficiencia y eficacia de una institución.

En su respuesta, la Municipalidad de Diego de Almagro señaló que se dispondrán las medidas necesarias para que los nuevos activos de tecnologías de la información sean ingresados al sistema de activo fijo para disponer de un registro único por elemento de forma individualizada y de esta forma poder revisar, controlar e identificar este tipo de bienes.

Asimismo, la entidad indicó evaluar la modificación del reglamento interno municipal, teniendo en cuenta las tecnologías de la información con el fin de asignar dichas funciones al Departamento de Informática.

Según lo anterior, se mantienen las observaciones, dado que las gestiones anunciadas por el servicio, tendientes a subsanar las situaciones detectadas corresponden a acciones futuras no materializadas a la fecha, por lo cual la entidad deberá, en un plazo no superior a 60

días hábiles contados a partir de la recepción del presente informe, remitir el inventario de los activos computacionales -hardware y software-, debidamente registrados con códigos de inventario asignados por la institución.

II. EXAMEN DE LA MATERIA AUDITADA

3. Encargado y Comité de Seguridad.

3.a) Falta de designación Encargado de Seguridad de la Información.

Se constató que el municipio no ha designado formalmente a un funcionario que cumpla las labores como Encargado de Seguridad de la Información, lo que imposibilita el desarrollo de políticas de seguridad, el asesoramiento a los diferentes departamentos que conforman la entidad comunal y que requieran de procedimientos tecnológicos, que participe en la coordinación de respuesta ante incidentes que afecten a los activos de información institucional y en la sensibilización de la aludida seguridad a los funcionarios de la repartición, entre otras funciones, situación que fue corroborada por don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro mediante correo electrónico de fecha 13 de agosto de 2021.

Al respecto, es preciso señalar que no se ha dado cumplimento a lo estipulado en el artículo 12 del decreto supremo N° 83, de 2004, antes citado, que establece que debe existir un encargado de seguridad, que actuará como asesor del jefe de servicio en los asuntos relativos a la seguridad de los documentos electrónicos, además de otras funciones en relación con políticas de seguridad.

En su respuesta, la autoridad comunal señaló que designará un funcionario que cumpla labores como Encargado de Seguridad de la Información y que actuará como asesor del jefe de servicio en políticas de seguridad.

Referente a este punto, se mantienen las observaciones, debido a que las gestiones anunciadas, no se han materializado, por lo cual la entidad deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir la designación formal del Encargado de Seguridad de la Información.

3.b) Inexistencia de un Comité de Seguridad de la Información.

Se verificó que el municipio no cuenta con un Comité de Seguridad de la Información, lo que impide, 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 y analizar incidentes de seguridad; y aprobar iniciativas para mejorar las operaciones informáticas, entre otros aspectos, hecho que fue ratificado por don [redacted], Jefe del Departamento

de Informática de la Municipalidad de Diego de Almagro mediante correo electrónico de fecha 13 de agosto de 2021.

Lo indicado en el párrafo precedente transgrede lo contenido en el artículo 37, la letra b) del referido decreto N° 83, de 2004, sobre Seguridad Organizacional, y los numerales 6.1.1 y 6.1.2, de la Norma Técnica NCh-ISO N° 27.002, de 2009, que disponen que la dirección debería 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 y que las actividades referentes a la seguridad de la información deberían ser coordinadas por representantes de diferentes partes de la organización con funciones y roles pertinentes.

En su respuesta, la entidad municipal señaló que definirá representantes de diferentes partes de la organización con funciones y roles pertinentes para conformar el Comité de Seguridad de la Información.

Según lo anterior, se debe mantener lo observado, dado que las medidas comprometidas aún no se han concretado, por lo cual el servicio deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir la designación formal del Comité de Seguridad de la Información.

4. Política de seguridad.

4.a) Ausencia de política de seguridad de la información.

Se corroboró que la entidad comunal no ha establecido una política de seguridad de la información que cumpla con los estándares estipulados en el artículo 11, del mencionado decreto N° 83, de 2004, el que señala en su inciso primero 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.

Asimismo, no se aviene a lo previsto en el numeral 5 de la NCh ISO 27.002, de 2009, que dispone que la dirección debería establecer una orientación clara de la política en la línea con los objetivos de negocio y demostrar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización.

A su vez, infringe el artículo 3°, inciso segundo, de la citada ley N° 19.880, que define al acto administrativo como la decisión formal que emitan los órganos de la administración del estado en los cuales contienen declaraciones de voluntad, realizadas en el ejercicio de una potestad pública, el que de acuerdo con el principio de escrituración, contemplado en el artículo 5° del mismo texto legal, se expresará por escrito.

En su respuesta, la Municipalidad de Diego de Almagro señaló que, una vez conformado el Comité de Seguridad de la Información, se deberán aprobar las políticas de seguridad, conocer los riesgos a los cuales se encuentran expuestos los activos de información, revisar y analizar incidentes de seguridad y aprobar iniciativas para mejorar las operaciones informáticas, entre otros aspectos.

Referente a este punto, se mantienen las observaciones, debido a que las gestiones anunciadas, no se han materializado, por lo cual la entidad deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir la política de seguridad de la información.

4.b) Contenido de la política de seguridad de la información.

Se constató, que si bien, la entidad dispone de un manual de procedimientos de Informática, aprobado a través del Acuerdo N° 100 del Concejo Municipal de Diego de Almagro, de fecha 22 de mayo del año 2012, se advirtió que tal documento no cumple con los requisitos mínimos exigidos en el artículo 11 del citado decreto N° 83, de 2004 para ser considerado como una política de seguridad de la información, a saber: Una definición de seguridad del documento electrónico, sus objetivos globales, alcance e importancia; la difusión de sus contenidos al interior de la organización y su reevaluación en forma periódica, a lo menos cada 3 años.

Asimismo, tampoco se condice con los requisitos establecidos en los numerales 5.1.1. y 5.1.2. de la NCh ISO 27.002, de 2009, que dispone que el documento con la política de seguridad de la información debería contener declaraciones respecto de: definición de la seguridad de la información, sus objetivos, alcances generales y la importancia de la seguridad como mecanismo que permite compartir la información; una declaración de la intención de la dirección, apoyando los objetivos y principios de la seguridad de la información alineada con las estrategias y objetivos de negocio; un marco para fijar objetivos de control y controles, incluyendo la estructura de evaluación y gestión del riesgo; una breve explicación de las políticas, principios, normas y requisitos de seguridad de la información; una definición de responsabilidades generales y específicas en materia de gestión de la seguridad de la información, incluida la comunicación de los incidentes relativos a la seguridad; las referencias a la documentación que pueda sustentar la política; por ejemplo, políticas y procedimientos mucho más detallados para sistemas de información específicos o las reglas de seguridad que los usuarios deberían cumplir.

En su respuesta, la entidad municipal señaló que deberá elaborar un documento que cumpla con los requisitos mínimos exigidos en el artículo 11 del decreto Nº 83 de 2004 sobre seguridad organizacional, a saber: una definición de seguridad del documento electrónico, sus objetivos globales, alcance e importancia, la difusión de sus contenidos al interior de la organización y su reevaluación en forma periódica (cada 3 años).

De acuerdo con lo anterior se debe mantener lo observado, dado que las medidas comprometidas aún no se han concretado, por lo

cual el servicio deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir la política de seguridad de la información.

4.c) Incumplimientos manual de procedimientos de informática.

4.c.a) Referente al proceso de adquisición e instalación de equipos.

De conformidad con lo señalado por don [redacted], Jefe del departamento de Informática de la Municipalidad de Diego de Almagro a través de una entrevista realizada por medio de la plataforma Teams el día 25 de agosto de 2021, se pudo advertir que no todos los equipos adquiridos por la entidad edilicia son instalados por el área de informática.

La situación planteada vulnera lo contenido en el inciso 3° del apartado “Adquisición de equipos” del mencionado manual de procedimientos de informática que dispone que es de responsabilidad del Departamento de Informática la instalación de equipos computacionales, como también la realización de las pruebas técnicas respectivas.

En su respuesta, el municipio señaló que deberá revisar y actualizar el manual de procedimientos de informática y al establecer las políticas de seguridad de la información se redefinirán las responsabilidades de instalación, habilitación, configuración e implementación de recursos necesarios para velar por el buen uso y funcionamiento del equipamiento entregado por el servicio.

Referente a este punto, se mantienen las observaciones, debido a que las gestiones anunciadas, no se han materializado, por lo cual la entidad deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir un documento oficial que señale las responsabilidades sobre la adquisición, registro del inventario, instalación, habilitación, configuración e implementación de recursos informáticos.

4.c.b) Respecto del uso del correo institucional.

Se constató que el municipio no ha realizado labores de difusión y/o capacitaciones respecto de los riesgos asociados al uso del correo electrónico institucional establecidos en el apartado “Procedimientos uso de correo del correo electrónico” del referido manual de procedimientos de informática, situación que fue ratificada por don [redacted] Jefe del Departamento de Informática de la entidad edilicia a través de entrevista realizada por la plataforma TEAMS el día 25 de agosto de 2021.

Lo anteriormente expuesto denota un incumplimiento a lo establecido en el artículo 11 de la ley N° 18.575, Orgánica Institucional de Bases para la Administración del Estado, en cuanto a que las autoridades y jefaturas, dentro de un ámbito de su competencia y en los niveles que corresponda, ejercerán un control jerárquico permanente del funcionamiento de los organismos y de la actuación del personal de su dependencia.

En su respuesta, el servicio señaló que deberá generar espacios de comunicación, difusión y/o capacitación sobre los riesgos asociados al uso del correo electrónico institucional conforme a lo expuesto en el manual de procedimientos de informática e incluirlos dentro de las políticas de seguridad de la información.

Según lo anterior, se mantienen las observaciones, dado que las gestiones anunciadas por el servicio, tendientes a subsanar las situaciones detectadas corresponden a acciones futuras no materializadas a la fecha, por lo cual la entidad deberá remitir, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, los respaldos de las difusiones y/o capacitaciones realizadas con respecto de los riesgos asociados al uso del correo electrónico institucional.

4.d) Información no proporcionada.

Sobre el particular, es preciso indicar que mediante correo electrónico de fecha 26 de agosto de 2021 se solicitó a la entidad comunal los antecedentes que respalden las últimas 5 solicitudes de alta/baja o cambio de cuentas de usuario de SIFIM, a fin de acreditar el cumplimiento de formato y de forma señalados en el manual de procedimientos dispuesto para tales fines.

Al respecto, cabe hacer presente que don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro, por medio de correo electrónico de fecha 26 de agosto de 2021, como respuesta al requerimiento, proporcionó acceso a una carpeta compartida a través de Google drive, el cual incluía, entre otros, una carpeta denominada “4. Solicitudes de alta, baja, modificaciones”, que no contenía los antecedentes solicitados.

La situación señalada vulnera lo prescrito en el artículo 17 de la mencionada resolución N° 10, de 2021, que indica, en lo que interesa, que la entidad o servicio auditado proporcionará los accesos a las bases de datos y antecedentes requeridos en los plazos definidos.

A su vez lo descrito no se condice con lo previsto en los artículos 3° y 8° de la indicada ley N° 18.575, que señala que es deber de observar los principios de responsabilidad, eficiencia, eficacia, y de accionar por propia iniciativa en el cumplimiento de sus funciones, procurando la simplificación y rapidez de los trámites.

En su respuesta, la entidad municipal señaló que las últimas 5 solicitudes de alta/baja y/o modificación de usuarios SIFIM que acreditaban el cumplimiento del formato y la forma señalado en el manual fueron olvidados de cargar, sin embargo cabe mencionar que aún hay direcciones en las cuales se está trabajando para dar un mejor entendimiento al proceso de solicitud en cuanto a formato y forma se refiere.

De acuerdo con lo anterior se debe mantener lo observado, pues si bien la entidad da cuenta de los motivos sobre la información no

proporcionada, no adjunta los documentos que permitan su subsanación, por lo cual el servicio deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir las últimas 5 solicitudes de alta/baja y/o modificación de usuarios SIFIM debidamente regularizadas o presentar un documento oficializado que actualice lo descrito en el manual de procedimiento para el alta, baja y cambio de usuarios que trabajan con los Sistemas de Información Financiera Municipal, SIFIM, y Mercado Público, autorizado mediante acta de acuerdo N° 79, del Concejo Municipal, de fecha 8 de mayo de 2012.

5. Gestión de riesgos.

5.a) Ausencia de evaluación de riesgos.

Se constató que la entidad edilicia no ha efectuado una evaluación de riesgos de seguridad, situación que fue ratificada por don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro mediante correo electrónico de fecha 13 de agosto de 2021.

Al respecto, cabe hacer presente que lo expuesto no se condice con lo establecido en el numeral 0.4, de la NCh ISO 27.002, de 2009, la cual señala que los requisitos de seguridad se identifican mediante una evaluación metódica de los riesgos. El gasto en controles se debería equilibrar con el perjuicio en el negocio, resultante de los fallos de seguridad.

Agrega, que los resultados de esta evaluación ayudarán a orientar y a determinar una adecuada acción gerencial y las prioridades para gestionar los riesgos de seguridad de la información, y la implementación de los controles seleccionados para proteger contra dichos riesgos.

En su respuesta, la Municipalidad de Diego de Almagro señaló que, si bien no se ha efectuado una evaluación de riesgos de seguridad formal, se están implementando metodologías de seguridad física y digital que minimicen los riesgos asociados, las cuales deberán ser evaluadas, ratificadas y autorizadas por el Comité de Seguridad de la información.

Referente a este punto, se mantienen las observaciones, debido a que las gestiones anunciadas, no se han materializado, por lo cual la entidad deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir el informe de evaluación de riesgos.

6. Clasificación y control de bienes.

De la revisión efectuada a la información contenida en el inventario de activos de las tecnologías de información, se determinó lo siguiente:

6.a) Catastro de activos de tecnologías de la información incompleto y desactualizado.

Se constató que el Departamento de Informática mantiene un catastro de los equipos del Municipio listados en planilla Excel y en documentos físicos (formularios utilizados en la labor de soporte técnico del área), sin embargo, la información contenida en ellos se encuentra desactualizada por cuanto se registran equipos dados de baja, en circunstancias que dichos bienes se encuentran siendo utilizados por un usuario en específico, así como tampoco registra el universo real de computadores con sus usuarios asignados. El detalle se expone en anexo N° 2.

Asimismo, se pudo verificar que dicho reporte no incluye los códigos de inventario asignados por la institución y que además no se incorpora el registro de otros dispositivos, como es el caso de los mouses, cargadores de notebook, u otro elemento asociado a las tecnologías de la información, lo que impide la adecuada revisión, control e identificación inmediato de este tipo de bienes.

En su respuesta, la entidad edilicia señaló que se dispondrán las medidas necesarias para que los nuevos activos de tecnologías de la información sean ingresados al sistema de activo fijo para así disponer de un método de seguimiento del activo desde su adquisición y/o movimientos de dependencias hasta su baja.

Según lo anterior, se mantienen las observaciones, dado que las gestiones anunciadas por el servicio, tendientes a subsanar las situaciones detectadas corresponden a acciones futuras no materializadas a la fecha, por lo cual la entidad deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir el catastro de equipos computacionales del departamento de Informática actualizado y con las correcciones necesarias para subsanar la observación.

6.b) Ausencia de un catastro de software en inventario de activos de tecnologías de la información.

Se pudo corroborar, que el catastro de informática no contiene el inventario de los softwares- el cual corresponde al listado de programas considerados como oficiales por el municipio- tanto de aquellos adquiridos como de los instalados, así como tampoco se registra la cantidad de licencias por software.

Las situaciones planteadas en los numerales 6.a) y 6.b) no dieron cumplimiento a lo dispuesto en los artículos 13, 14, 15 y 16 del citado decreto N° 83, de 2004, en relación con la clasificación, control y etiquetado de bienes.

Además, transgreden el numeral 12.6.1 de la Norma Técnica NCh-ISO N° 27.002, de 2009, del Instituto Nacional de Normalización, el que estipula que, el requisito previo para la gestión eficaz de vulnerabilidades técnicas en una institución es un inventario actualizado y completo de los activos. Esta información específica es necesaria para apoyar la gestión de vulnerabilidades técnicas, incluye al vendedor de software, números de versión, el

estado actual de despliegue (por ejemplo, qué software está instalado sobre qué sistemas), y las personas responsables dentro de la organización.

En su respuesta, el servicio señaló que se diseñará una metodología que permita ingresar la adquisición del software y sus respectivas habilitaciones y movimientos, además de la administración realizada por las plataformas propietarias (Microsoft, Autodesk, entre otras).

De acuerdo con lo anterior se debe mantener lo observado, dado que las medidas comprometidas aún no se han concretado, por lo cual el servicio deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir el catastro de software que incluya las licencias adquiridas y las instaladas, indicando el usuario que le fue asignado.

6.c) Inconsistencias en el catastro de activos de tecnologías de la información.

Se constató que un total de 6 computadores, la información registrada en el inventario difiere de lo real, respecto del funcionario asignado, de su ubicación y del área, según el detalle se encuentra en el anexo N° 3, del presente informe.

Del mismo modo, se corroboró que el equipo computacional genérico, serie N° 00180464762866, de nombre “CONTABILIDAD-01”, asignado actualmente a la funcionaria Carolina González Yáñez, mantiene instalado el sistema operativo Windows 10 Profesional instalado, el cual difiere de lo informado en la muestra que corresponde a Windows 7 Profesional.

Cabe destacar, que los puntos anteriormente observados, no dieron cumplimiento a lo dispuesto en los artículos 13, 14, 15 y 16 del decreto N° 83, de 2004, antes individualizado, en relación con la clasificación, control y etiquetado de bienes.

Asimismo, lo señalado precedentemente, no se condice con lo establecido en el numeral 12.6.1 de la Norma Técnica NCh-ISO 27.002, de 2009, que estipula que el requisito previo para la gestión eficaz de vulnerabilidades técnicas en una institución es un inventario actualizado y completo de los activos. Esta información específica es necesaria para apoyar la gestión de vulnerabilidades técnicas, incluye al vendedor de software, números de versión, el estado actual de despliegue, y las personas responsables dentro de la organización.

En su respuesta, la Municipalidad de Diego de Almagro señaló que si bien el método actual permite el ingreso de los activos y sus características, este se complica al momento de registrar algún movimiento o cambio en el personal asignado, ya que estos no siempre son informados y/o realizados por el departamento de informática. Esta mejora se verá reflejada al momento de habilitar el sistema de activo fijo. Respecto a las actualizaciones de sistemas operativos no es posible evitar que estas ocurran dada la configuración actual del proveedor Microsoft las cuales son automáticas.

Referente a este punto, si bien el servicio indica que no es posible evitar las actualizaciones de los sistemas operativos, debe entenderse en su contexto, que la observación está definida hacia los controles preventivos de actualización del catastro con respecto a estas actualizaciones, como por ejemplo: revisiones periódicas, coordinaciones entre unidades, difusiones u otro mecanismo preventivo que favorezca la gestión eficaz de los activos.

La entidad indica a su vez, acciones futuras para llevar un control sobre los movimientos de personal, por lo que se debe mantener lo observado, debiendo, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir el catastro de equipos con todas las correcciones necesarias para subsanar la observación.

7. Control de accesos.

7.a) Sobre configuración cuentas de usuarios en Windows con privilegios de administrador.

De la revisión a los permisos establecidos a cada cuenta de usuario en Windows, se pudo constatar que un total de 17 cuentas se encuentran configuradas con privilegios de administrador, lo que constituye un riesgo a la seguridad, como la modificación de la configuración del sistema operativo, mayores daños provocados por virus, instalación de software no autorizado, entre otros. Los detalles se muestran en anexo N° 4.

Además, la situación antes descrita denota una falta de segregación de funciones por parte del municipio respecto de la asignación de privilegios para la configuración de sus sistemas y los usuarios involucrados.

Lo expuesto incumple lo establecido en el artículo 23, del mencionado decreto N° 83, en armonía con lo estipulado en el numeral 10.1.3, de la NCh-ISO Nº 27.002, de 2009, los que disponen que, para reducir el riesgo o mal uso de los sistemas, deberán aplicarse políticas de segregación de funciones.

En su efecto, la letra c) del numeral 11.2.1 de la NCh-ISO Nº 27.002, de 2009, menciona que el nivel de acceso otorgado debe ser apropiado para el propósito del negocio y consistente con la política de seguridad, por ejemplo, que no comprometa la segregación de tareas.

En su respuesta, la entidad municipal mencionó que el equipamiento listado en el anexo N° 4 corresponde a equipos con sistemas CAS-Chile habilitado, el cual según instrucciones del proveedor requiere el uso a través de una cuenta con privilegios de administrador, ya que los sistemas deben registrar las transacciones realizadas, imprimir informes y tener permisos de escritura en la unidad C:\ de sistema para crear los logs de uso como también dentro de los registros de sistema. Se estudiará en las políticas de seguridad y con el comité.

Según lo anterior, la respuesta del servicio no es suficiente para subsanar la observación, pues conforme a la validación sobre la muestra de equipos computacionales, se determinó que los computadores asignados a los usuarios [redacted] no tienen instalado el sistema Cas Chile y sin embargo mantienen cuenta con privilegios administrativos.

Por otra parte, la entidad municipal no adjunta respaldos que provengan del proveedor Cas Chile los cuales indiquen, como requisito de operación, el manejo de cuentas de usuario del sistema operativo Windows con privilegios de administrador, por lo que se deben mantener las observaciones, debiendo el servicio, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir la aclaración por los cuatro equipos computacionales asignados a los usuarios [redacted] los cuales no tienen instalado el sistema Cas Chile y sin embargo mantienen cuenta con privilegios administrativos, y además, remitir un documento que certifique la instrucción del proveedor CAS Chile con la configuración de las cuentas de usuario Windows para el manejo de sus sistemas.

7.b) Sobre utilización de cuentas de usuarios genéricas en Windows.

Se advirtió, que en 17 casos el servicio no configuró a los usuarios del sistema operativo Windows utilizando una identificación única de usuario (IDs), por lo cual los funcionarios ingresan con una cuenta de usuario genérica y conocida. El detalle se encuentra en el anexo N° 5.

En su respuesta, el servicio señaló que debido a los constantes movimientos de personal municipal en cada área y el déficit de personal de soporte para atender cada requerimiento de configuración en cuanto a equipamiento se refiere, se mantiene un procedimiento de reasignación de clave a cada usuario y/o modificación cuando este es reasignado, ya que el equipamiento no se traslada con el funcionario sino que pertenece al área asignada; El equipo conserva la data de respaldo propiedad de cada dirección a menos que se solicite lo contrario.

De acuerdo con lo anterior se debe mantener lo observado, pues el procedimiento que el servicio describe en su respuesta no se ajusta a la normativa que da origen a la observación señalada, por lo cual el servicio deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, dar cuenta de la regularización de los 17 casos observados, a través de una captura de pantalla de la cuenta de usuario donde se identifique el funcionario que tiene asignado el equipamiento.

7.c) Sobre irregularidades en las cuentas de usuarios en sistema SIFIM.

Del análisis a las cuentas de usuario del Sistema denominado SIFIM, se evidenció, la existencia de 58 casos con identificadores genéricos (ID de usuario), 36 casos de identificadores asignados a

un responsable genérico y 6 casos de identificadores asignados un responsable distinto, tal como se expone en el anexo N° 6.

Las situaciones planteadas en los numerales 7.b) y 7.c), incumplen lo establecido en el artículo 27, 28, 29, 30 y 32 del citado decreto N° 83, sobre el uso de identificadores y del numeral 11.2.1, letra a) de la NCh-ISO Nº 27.002, de 2009, la cual señala que la utilización de la identificación única de usuario (IDs) es para permitir que los usuarios queden vinculados y sean responsables de sus acciones; el uso del identificador de grupo, se debería permitir solamente cuando sea necesario por razones de negocio u operativas, y deberían ser aprobadas y documentadas.

Luego, el numeral 11.5.2 dispone que todos los usuarios deberían tener un identificador único (ID de usuario) para su uso personal exclusivo, y se debería elegir una técnica de autenticación adecuada para sustentar la identidad alegada por un usuario.

En su respuesta, la Municipalidad de Diego de Almagro señaló que las cuentas en mención se encuentran fuera de servicio o pertenecen a otra institución, ya que las bases de datos fueron cargadas por el proveedor CAS-Chile a través de una réplica de otro municipio, por lo que muchas de esas cuentas no pertenecen a la institución, ni siquiera existen las unidades que allí se mencionan, ni los sistemas. Se realizará levantamiento de usuarios y se eliminarán las cuentas no solicitadas y no pertenecientes al municipio.

Referente a este punto, se mantienen las observaciones, debido a que las gestiones anunciadas, no se han materializado, por lo cual la entidad deberá remitir, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, una nueva nómina en formato Excel (xls o xlsx) con las cuentas de usuario del Sistema SIFIM, en donde se evidencie las modificaciones y/o eliminaciones, además de un certificado firmado que respalde el archivo digital.

7.d) Respecto de la configuración de contraseñas.

Se constató que las contraseñas de SIFIM no están conformadas con un mínimo de ocho caracteres, ni tampoco la entidad comunal valida que éstas se encuentren libres de caracteres idénticos, consecutivos o grupos completamente numéricos o alfabéticos, situación que fue corroborada por don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro a través de entrevista realizada vía Teams el día 25 de agosto del presente año.

La situación expuesta vulnera lo establecido en la letra g) del artículo 28 del aludido decreto N° 83, de 2004, el cual indica que los identificadores dispondrán de una longitud mínima de ocho caracteres; sean fáciles de recordar; contengan letras, mayúsculas, dígitos, y caracteres de puntuación; no estén basados en cosas obvias o de fácil deducción a partir de datos relacionados con la persona, por ejemplo, nombres, números telefónicos, cédula de identidad, fecha de nacimiento; estén libres de caracteres

idénticos consecutivos o grupos completamente numéricos o alfabéticos; y no sean palabras de diccionario o nombres comunes. Agrega, en base a la misma materia, que los sistemas informáticos deberán configurarse de manera que los usuarios se vean compelidos a cumplir con las obligaciones detalladas en la norma.

En su respuesta, la Municipalidad de Diego de Almagro señaló que se validará con proveedor de sistemas la posibilidad de aumentar caracteres permitidos, ya que, dado que la creación de cuentas solo permitía el ingreso de 6 caracteres se procedió a generar las cuentas con 2 letras y 4 números aleatorios no consecutivos ante estos requerimientos, por lo que no se estaría cumpliendo el mínimo de 8 caracteres.

Según lo anterior, se mantienen las observaciones, dado que las gestiones anunciadas por el servicio, tendientes a subsanar las situaciones detectadas corresponden a acciones futuras no materializadas a la fecha, por lo cual la entidad deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir las gestiones realizadas con el proveedor de sistemas para modificar la extensión y complejidad de las contraseñas para dar cumplimiento de la normativa.

7.e) Sobre período de actualización de contraseñas.

De la revisión efectuada, se detectó la omisión del cambio periódico de las contraseñas de los usuarios en Windows y en SIFIM, dado que los sistemas no obligan a los usuarios a cambiar sus contraseñas después de un período determinado, vulnerando con ello, el artículo 28, la letra h) del mencionado decreto N° 83, y del numeral 11.3.1, la letra e) de la NCh-ISO Nº 27.002, de 2009, que indican que todos los usuarios deberían ser advertidos en cuanto al deber de cambiar los identificadores a intervalos regulares, asimismo que las contraseñas de accesos privilegiados se deberán cambiar más frecuentemente que los identificadores normales y evitar la reutilización o reciclaje de claves viejas.

En su respuesta, la entidad municipal señaló que, dado que no existen políticas de seguridad implementadas en los equipos, en situaciones que la dirección requiere acceder a la documentación de algún equipo específico en ocasiones ha sucedido que solo la persona encargada dispone de la contraseña de acceso por lo que se optó por bloquear la posibilidad de cambiar las claves asignadas. Se evaluará con el comité y en las políticas de seguridad para cada tipo de equipamiento conforme a sus características individuales y al uso que se le dará dentro del servicio.

De acuerdo con lo anterior se debe mantener lo observado, dado que las medidas comprometidas aún no se han concretado, por lo cual el servicio deberá definir el procedimiento para cambiar los identificadores a intervalos regulares y comunicar, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, las adecuaciones en la plataforma tecnológica.

7.f) Equipos computacionales con acceso liberado.

Se constató que un total de 17 equipos computacionales mantienen acceso liberado de internet, en los cuales los funcionarios pueden acceder a redes sociales, no obstante, por su función efectiva no se justifica tal acceso. Lo anterior se detalla en anexo N° 7.

Tal situación, vulnera el artículo 33 del antes citado decreto N° 83, de 2004, y el numeral 11.4.1 de la norma NCh-ISO 27.002, la cual indica que los usuarios sólo deberían tener acceso a los servicios para cuyo uso están específicamente autorizados, lo que no aconteció en la especie.

En su respuesta, el servicio señaló, que se encuentra en proceso de habilitación de un equipo cortafuego (firewall) el cual permitirá solventar estos inconvenientes a nivel de red.

Según lo anterior, se mantienen las observaciones, dado que las gestiones anunciadas por el servicio, tendientes a subsanar las situaciones detectadas corresponden a acciones futuras no materializadas a la fecha, por lo cual la entidad deberá remitir, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, las capturas de pantalla que den cuenta de la identificación del usuario y el bloqueo de redes sociales.

8. Control de acceso remoto

La entidad auditada no cuenta con administración de usuarios y licencias de VPN, no existiendo observaciones en este apartado.

En su respuesta, el servicio comentó que con la adquisición del firewall en mención en el punto anterior, se incorporará el uso de VPN administrado por la unidad de informática.

9. Seguridad física y del ambiente.

Sobre el particular, es del caso indicar que mediante correo electrónico de fecha 13 de agosto de 2021, el Jefe de Informática, don [redacted], proporcionó un registro fotográfico de las dependencias de la entidad auditada, ello, con el propósito de verificar el estado de las instalaciones donde se encuentran los equipos de comunicaciones y servidor SIFIM, así como también los controles de acceso y el perímetro de seguridad establecido para la sala donde se mantienen estos activos, determinando las siguientes observaciones:

9.a) Ausencia de bitácoras de acceso a sala de servidores.

Se constató que la sala de servidores no dispone de una bitácora o registro de acceso a las instalaciones, lo que incumple lo

contenido en el numeral 9.1.2, letra b) del de la Norma Chilena N° 27.002, de 2009, la cual especifica que el acceso a las áreas donde se procesa o se almacena la información sensible debería ser controlado y restringido sólo a las personas autorizadas; se deberían usar controles de autentificación, por ejemplo, tarjetas con número de identificación personal (PIN), para autorizar y validar el acceso; se debería mantener en forma segura una pista auditable de todos los accesos.

En su respuesta, la Municipalidad de Diego de Almagro señaló que el acceso no se encuentra restringido dadas 2 situaciones: 1) la sala de telecomunicaciones donde se encuentra el rack no dispone de un sistema de ventilación y/o refrigerante que permita la adecuada temperatura para el equipo allí instalado, es por esto que se está tramitando el cambio del equipo de condensado en mal estado a fin de mantener un ambiente seguro para el equipamiento instalado. 2) El acceso a la sala de telecomunicaciones solo es posible a través de la oficina de informática de la cual solo tiene acceso el encargado, el señor [redacted] y la dirección a la que pertenece la unidad de Informática, con respaldo en la Dirección de Obras quien recepcionó la ampliación del edificio.

Sin perjuicio de lo indicado por el servicio, referido a que el acceso a la instalación es a través de la oficina de informática, y ésta se encuentra resguardada con llave, se debe mantener lo observado, pues se debe hacer mención que el numeral 9.1.2, letra a) del de la Norma Chilena N° 27.002, de 2009, propone mantener el registro de la fecha y hora de entrada y salida de los visitantes, concedidos sólo para propósitos especificados y autorizados, por lo que el servicio deberá remitir, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, la evidencia de la puesta en marcha de una bitácora física.

9.b) Inexistencia de puerta de cortafuego.

Se advirtió que la sala del área de comunicaciones no dispone de una puerta cortafuego, situación que incumple el numeral 9.1.1 letra e) de la Norma Chilena N° 27.002, la cual considera la implementación de puertas contra incendios, las que deberían funcionar de acuerdo con las disposiciones locales de protección contra el fuego de modo de garantizar la seguridad. El registro fotográfico se muestra en el anexo N° 8, Fotografía N° 1.

En su respuesta, la entidad municipal señaló que deberá se evaluará con el Comité de Seguridad.

De acuerdo con lo anterior se debe mantener lo observado, dado que las medidas comprometidas aún no se han concretado, por lo cual el servicio deberá remitir, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, un plan de mejora para la sala de servidores que atienda a lo indicado en la observación.

9.c) Inexistencia de sistemas de emergencia en sala de servidores.

Se comprobó que la sala de servidores no cuenta con sistemas de emergencia, tales como detectores de humo, alarmas, u otro tipo de sensores, infringiendo con ello del numeral 9.2.1, la letra d) de la Norma Chilena N° 27.002, que expone que, se deberían adoptar controles para reducir al mínimo el riesgo de amenazas físicas potenciales, como ser: hurto, fuego, explosivos, humo, inundaciones, polvo y vibraciones, efectos químicos, interferencias en el suministro eléctrico, interferencia de las comunicaciones, radiación electromagnética y vandalismo.

En su respuesta, el servicio señaló que existe regulador de voltaje conectado a la línea eléctrica de la sala, los demás sistemas se evaluarán con el comité de seguridad.

Referente a este punto, se mantienen las observaciones, debido a que las gestiones anunciadas, no se han materializado, por lo cual la entidad deberá remitir, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, un plan de mejora para la sala de servidores que atienda a lo indicado en la observación.

9.d) Falta de sistema de iluminación de emergencia.

Se observó que la sala de servidores no cuenta con iluminación de emergencia en casos de contingencia, situación que transgrede el numeral 9.2.2 de la Norma Chilena N° 27.002, el que manifiesta que, se debería proteger el equipamiento contra posibles fallas en el suministro de energía y otras interrupciones causados por fallas en elementos de soporte.

En su respuesta, la entidad comunal señaló que se evaluará con el Comité de Seguridad.

De acuerdo con lo anterior, se mantiene la observación, debido a que las gestiones anunciadas, no se han materializado, por lo cual la entidad deberá remitir, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, un plan de mejora para la sala de servidores que permita habilitar la instalación con iluminación de emergencia.

9.e) Sobre señalética en sala de servidores.

Se evidenció que la sala de servidores no cuenta con carteles en lugares visibles que establezcan las prohibiciones de fumar, consumir alimentos y/o bebidas, situación que no se ajusta a lo dispuesto en el artículo 18, letra a) del mencionado decreto N° 83, de 2004, que señala que, cada órgano deberá impartir y publicitar instrucciones relativas al consumo de alimentos, bebidas y tabaco en las cercanías de sistemas informáticos, como asimismo, en lo establecido en el numeral 9.2.1, letra e) de la NCh ISO 27.002, de 2009.

En su respuesta, la municipalidad señaló que se implementará la señalética en mención.

De acuerdo con lo anterior se debe mantener lo observado, dado que las medidas comprometidas aún no se han concretado, por lo cual el servicio deberá remitir, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, las fotografías que den cuenta de la habilitación de estos carteles en lugares visibles que establezcan las prohibiciones de fumar, consumir alimentos y/o bebidas.

9.f) Referente a equipo de ventilación en sala de servidores.

Se observó que el equipo de aire acondicionado instalado en la sala de servidores se encuentra sin funcionamiento, desde su falla acontecida a un año de su instalación, esto es, en el año 2017, situación que se mantiene a octubre de 2021. La entidad edilicia no ha reparado este equipo ni ha implementado otro mecanismo que pueda proveer de acondicionamiento de la sala para minimizar el riesgo de posibles amenazas ambientales como lo es la temperatura, que pudiera afectar adversamente a la operación de los equipos instalados.

La situación antes descrita, vulnera lo establecido en el numeral 9.2.1, letra f) de la NCh ISO 27.002, de 2009, el cual dispone que las condiciones ambientales, tales como temperatura y humedad, se deberían supervisar para verificar que las mismas no afectan negativamente el funcionamiento de las instalaciones de procesamiento de la información. El registro fotográfico se muestra en el anexo N° 8, Fotografía N° 2.

En su respuesta, el servicio señaló que se encuentra en proceso la adquisición de un equipo nuevo de condensado en reemplazo del que se encuentra en mal estado revisado por empresa externa al realizar la mantención solicitada y realizada en diciembre de 2021.

De acuerdo con lo anterior se debe mantener lo observado, dado que las medidas comprometidas aún no se han concretado, por lo cual el servicio deberá remitir, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, el estado de habilitación y funcionamiento del equipo de aire acondicionado para subsanar la observación.

9.g) Sobre seguridad implementada en sala de servidores.

Se constató que no existen alarmas en los accesos de la sala de servidores y además la puerta de la sala permanece abierta por temas de ventilación lo cual denota una falta de seguridad en el control de acceso.

Sobre el particular, cabe hacer presente, que la sala de servidores se encuentra dentro del departamento de informática, el cual se encuentra claramente definido, y que para acceder a ella, se debe tener llaves de la puerta del departamento de informática, [redacted]. El registro fotográfico se muestra en el anexo N° 8, Fotografía N^{os} 3 y 4.

Lo anteriormente expuesto no se ajusta a lo indicado en las letras b) y f) del numeral 9.1.1 de la Norma Chilena N° 27.002, que señala que, el perímetro de un edificio o un lugar que contenga instalaciones de procesamiento de información deberían estar protegidas, mediante mecanismos de control, por ejemplo, vallas, alarmas, cerraduras, entre otras.

En su respuesta, la entidad municipal señaló que la sala dispone [redacted].

Según lo anterior, se deben mantener las observaciones, dado que no se advierten cambios propuestos por el servicio tendientes a su subsanación, por lo cual la entidad deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir un plan de mejora para la sala de servidores que incluya la instalación de alarmas en los accesos y/o corregir la situación con el equipo de aire acondicionado, motivo por el cual a puerta de la sala permanece abierta por problemas de ventilación.

9.h) Sobre instalaciones eléctricas en sala de servidores.

Se constató que, la instalación eléctrica realizada para el funcionamiento del aire acondicionado de la sala de servidores no cumple con los estándares de seguridad, por cuanto el cable de energía se encuentra colgando en la pared, situación que vulnera la contenido en el numeral 9.2.3, letra a) de la NCh ISO 27.002, de 2009, la cual indica que las líneas de energía y telecomunicaciones en instalaciones de procesamiento de la información deben ser subterráneas, siempre que sea posible, o sujetas a una adecuada protección alternativa. El registro fotográfico se muestra en el anexo N° 8, Fotografía N° 2.

En su respuesta, el servicio señaló que se evaluará con el Comité de Seguridad.

De acuerdo con lo anterior, se mantiene la observación, debido a que las gestiones anunciadas, no se han materializado, por lo cual la entidad deberá remitir, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, un plan de mejora para la sala de servidores que incluya la correcta instalación del cableado del equipo de aire acondicionado.

9.i) Sobre implementación de bitácoras en sala de servidores.

Se constató que la repartición no posee bitácoras que refleje el detalle de fallas detectadas, o el cambio de equipamiento de la sala de servidores, así como tampoco cuenta con un registro del mantenimiento de los servidores y dispositivos de comunicación, lo que no se aviene con lo dispuesto en el numeral 9.2.4, la letra c) de la citada norma chilena NCh ISO 27.002, de 2009, la que indica que se deberían mantener registros de todas las fallas, reales o sospechosas, así como de todo el mantenimiento preventivo y correctivo.

En su respuesta, la entidad municipal señaló que se implementará el uso de bitácora de acceso a la sala quedando registrado el uso en las políticas de seguridad.

De acuerdo con lo anterior se debe mantener lo observado, dado que las medidas comprometidas aún no se han concretado, por lo cual el servicio deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir las fotografías que evidencien la puesta en marcha de una bitácora física.

9.j) Referentes a respaldos en el servidor.

Se constató, que los medios de respaldo locales del servidor SIFIM, no se localizan a una distancia prudente del emplazamiento principal, zona que debería ser definida e incluida en la política de respaldo, vulnerando lo contenido en el numeral 9.1.4, la letra b) de la NCh ISO 27.002 de 2009, la cual señala que el equipamiento en reserva y los medios de respaldo se deberían localizar a una distancia prudente para evitar daños producto de un desastre que afecten al emplazamiento principal.

En su respuesta, el servicio señaló que se evaluará con el Comité de Seguridad.

De acuerdo con su respuesta, se mantiene la observación, debido a que las gestiones anunciadas, aún no se han materializado, por lo cual la entidad deberá remitir, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, la política de respaldo debidamente formalizada que defina la zona ubicada a una distancia prudente del emplazamiento principal para el almacenamiento de los medios de respaldo locales del servidor SIFIM.

10. Gestión de las operaciones y las comunicaciones.

10.a) Procedimientos de destrucción de información.

La entidad edilicia no dispone de procedimientos formales relacionados con los procesos de destrucción de información de los equipos en desuso, pero da cuenta de procedimientos informales que el departamento de informática realiza sobre la materia, situación que fue corroborada mediante entrevista realizada el día 25 de agosto de 2021, a don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro a través de la plataforma TEAMS.

Lo indicado contraviene lo estipulado en el numeral 9.2.6 de la NCh ISO 27.002, de 2009, que señala que todo equipamiento que contenga medios de almacenamiento se debería revisar para asegurar que todos los datos sensibles y software licenciado se hayan removido o se hayan sobrescrito con seguridad antes de su disposición.

En su respuesta, el ente edilicio señaló que se incluirán políticas de destrucción de información de equipos en desuso en las políticas de seguridad.

Referente a este punto, se mantienen las observaciones, debido a que las gestiones anunciadas, no se han materializado, por lo cual la entidad deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir los procedimientos formales relacionados con los procesos de destrucción de información de los equipos en desuso.

10.b) Controles criptográficos.

Sobre el particular, es preciso indicar que la Municipalidad de Diego de Almagro mantiene un servidor que es parte del programa SIFIM de la Subsecretaría de Desarrollo Regional y Administrativo, en adelante SUBDERE, que aloja la base de datos del sistema de gestión financiero contable de CAS Chile, instalado sobre un motor de SQL Server 2008.

En este contexto, se constató que la información contenida en las tablas de datos no se encuentra encriptada, a diferencia de las contraseñas de los usuarios del sistema que si se encuentran encriptadas, situación que no se condice con el artículo 37, la letra f) de aludido decreto N° 83, de 2004, del Ministerio de Secretaría General de la Presidencia, como, asimismo, a lo dispuesto en el numeral 10.8.1, la letra g) y el numeral 12.3 de la NCh ISO 27.002 los cuales indican que se debe hacer uso de técnicas criptográficas, por ejemplo, para proteger la confidencialidad, integridad y autenticidad de la información.

En su respuesta, la entidad municipal señaló que los accesos a la información contenida en el servidor cuentan con una modalidad de conectividad encriptada por lo que la transmisión de esta a través de la red no puede ser descifrada sin los permisos correspondientes o a través de los perfiles de sistema.

Sin perjuicio de lo que la entidad indica en su respuesta, se debe mencionar que, en el contexto del control de auditoría, los controles criptográficos deben aplicarse a la información digital almacenada juntamente con la transmisión y la recepción de datos. Si bien el servicio cumple con el control en parte al mantener las claves de los usuarios de forma cifrada, debe definir cuál es la información que considera sensible y afecta a ser cifrada en la base de datos para proteger la confidencialidad, integridad y autenticidad de la información.

Dentro de este contexto, debe mantenerse la observación, por lo cual la entidad deberá definir y comunicar formalmente cuál es la información sensible afecta a ser cifrada en la base de datos del sistema SIFIM, o en su defecto, comunicar el respaldo de las gestiones con el proveedor de software para cifrar los datos contenidos en las tablas de datos.

11. Licencias de software.

Sobre la materia, es menester indicar que a través del decreto de pago N° 891, de fecha 6 de mayo de 2016, el municipio pagó al proveedor Magens S.A. un total de $39.442.984 por la adquisición de 145 licencias Microsoft Office Standard 2016, 12 licencias Microsoft Windows Professional 10, 55 licencias SQLCAL 2014 y 55 licencias Windows Server Cal 2012.

Ahora bien, de la revisión efectuada a las licencias instaladas de los equipos determinados en la muestra, se determinaron las siguientes observaciones:

11.a) Utilización de licencias de Microsoft Office no autorizadas.

Se constató, que un total de 12 computadores mantienen instalado Office Standard 2010, 2 computadores permanecen con Office Professional Plus 2010 y 1 computador con Office Standard 2007, cuyas versiones son distintas a las contempladas en el referido expediente de pago de licencias de Office, por lo que corresponden a software no licenciados. El detalle se contempla en el anexo N° 9.

En su respuesta, la Municipalidad de Diego de Almagro señaló que, conforme a la adquisición del licenciamiento a perpetuidad del software en mención cabe destacar que el proveedor en el portal de administración por volúmenes entrega la posibilidad de realizar el downgrade[6] de las versiones adquiridas por lo que el licenciamiento se encuentra habilitado para las versiones 2007, 2010, 2013 y 2016.

De acuerdo con lo anterior se debe mantener lo observado, pues el servicio no adjunta el respaldo que acredite su respuesta, por lo cual el servicio deberá remitir, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, el contrato con la empresa Microsoft que acredite la disponibilidad de las descargas para realizar el downgrade a los equipos informáticos del Municipio.

11.b) Compra de licencias de software Microsoft Office no instaladas.

En relación a las 145 licencias perpetuas de Office Standard 2016 OPL NL Gov, adquiridas por la Municipalidad de Diego de Almagro, a través del citado decreto de pago N° 891, se advirtió, que, en un total de 15 computadores, equivalentes a un 75% de la muestra, dichas licencias no se encontraban instaladas, toda vez que en los equipos informáticos mantienen una versión de software distinto al adquirido. El detalle se expone en el anexo N° 9.

En su respuesta, el servicio señaló que, el licenciamiento es válido para versiones anteriores a las adquiridas por lo que queda

[6] Acción de instalar una versión anterior de cualquier software.

pendiente de revisión el equipamiento que aún no se encuentra regularizado y evaluar factibilidad ya que aún existe equipamiento con más de 10 años de uso.

Los argumentos esgrimidos por la Municipalidad no son suficientes para desvirtuar lo objetado por esta Entidad de Control, toda vez que, la entidad comunal incurrió en pagos por concepto de software que no utilizó, pues conforme a los documentos de pago, la adquisición original correspondía a la versión 2016, última versión disponible en el año descrito, lo cual se da cuenta en el valor del producto. Desde esa fecha, y tal como explica la entidad comunal, el 75% de computadores de la muestra no cuenta con esta versión instalada, por lo cual el servicio deberá remitir, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, un plan de renovación de equipos computacionales que permitan la instalación del software adquirido, que incluya responsables y plazos concretos para su ejecución.

Además, ese Municipio deberá, en lo sucesivo, efectuar un análisis previo para establecer las compatibilidades necesarias entre su plataforma de hardware y software, a fin de evitar situaciones como las descritas y dar cumplimiento a los principios de eficiencia y eficacia que rigen a los Órganos de la Administración del Estado.

11.c) Utilización de otros softwares no autorizados.

Conforme a la revisión, se detectó que en 10 equipos computacionales se encuentra instalado software sin licencia tales como Adobe Acrobat XI Pro, Adobe Photoshop CS6, Adobe Audition 1.5, Microsoft Project Profesional 2010, Adobe Creative Suite Master Collection y Microsoft Visio Premium 2010.

En relación con lo anterior, es preciso mencionar que en 2 equipos computacionales se observaron los programas de descarga de archivos jdownloader y utorrent, los cuales favorecen el almacenamiento y uso de software no autorizado, además de conllevar riesgos a la seguridad de la red del municipio. Los detalles se contemplan en el anexo N° 10.

En su respuesta, la entidad municipal señaló que se revisará el equipamiento en mención y se regularizarán aquellos que no cumplan con las directrices emanadas del manual de procedimiento de informática y dispongan de software no autorizado y/o sin licenciamiento.

Según lo anterior, se mantienen las observaciones, dado que las gestiones anunciadas por el servicio, tendientes a subsanar las situaciones detectadas corresponden a acciones futuras no materializadas a la fecha, por lo cual la entidad deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir las capturas de pantalla del panel de control que evidencie la eliminación del software.

Las situaciones planteadas en los numerales 11.a), 11.b) y 11.c) no se condicen con lo establecido en el artículo 22, letra b), del citado decreto N° 83, de 2004, en donde señala que, en todos los

organismos sujetos a la presente norma, deberán explicitarse y difundirse las exigencias relativas al cumplimiento con las licencias de software y la prohibición del uso de software no autorizado.

Asimismo, lo anteriormente expuesto, vulnera lo contenido en los artículos 19 y 20 de la ley N° 17.336, sobre Propiedad intelectual, los que disponen que nadie podrá utilizar públicamente una obra del dominio privado sin haber obtenido la autorización expresa del titular del derecho de autor, entendiéndose por autorización el permiso otorgado por el titular del derecho de autor, en cualquier forma contractual, para utilizar la obra de alguno de los modos y por alguno de los medios que esta ley establece.

Asimismo, contraviene los principios de responsabilidad, eficiencia, eficacia, contenidos en los artículos 3° y 11 de la referida ley N° 18.575, según los cuales el control se extenderá tanto a la eficiencia y eficacia en el cumplimiento de los fines y objetivos establecidos, como a la legalidad y oportunidad de las actuaciones, añadiendo su artículo 5° que las autoridades y funcionarios deberán velar por la eficiente e idónea administración de los medios públicos y por el debido cumplimiento de la función pública.

Además, se advierte una transgresión a lo prescrito en el artículo 55 de la citada ley N° 18.575, que exige el empleo de medios idóneos de diagnóstico, decisión y control, para concretar, dentro del orden jurídico, una gestión en plena concordancia con los aludidos principios de eficiencia y eficacia, lo que no ha acontecido en la especie, toda vez que, no se han instalado la totalidad de licencias adquiridas en los computadores asignados a los funcionarios de la entidad edilicia.

A mayor abundamiento, es del caso recordar que los principios antes aludidos obedecen al logro de metas y al uso óptimo de los recursos estatales, respectivamente, con el propósito de alcanzar los objetivos públicos con el menor costo para la Administración (aplica criterio contenido, entre otros, en los dictámenes N^{os} 25.737, de 1995; 46.618, de 2000; 7.347, de 2013, y 88.553, de 2015, todos de la Contraloría General de la República).

12. Desarrollo y mantenimiento de sistemas.

12.a) Ambientes de producción y prueba.

Se constató que la Municipalidad de Diego de Almagro no ha implementado ambientes separados para producción (sistema en línea) y las pruebas de sus sistemas (ver numeral 13.b. Copias de seguridad), en el servidor SIFIM, el cual mantiene la base de datos del sistema CAS Chile, lo que no se aviene con lo señalado en el artículo 37, letra f), del referido decreto N° 83, de 2004, sobre gestión de las operaciones y comunicaciones, en relación con lo establecido en el acápite 10.1.4 , de la citada norma chilena, NCh ISO 27.002, de 2009, que dispone que, los aludidos recursos para desarrollo, prueba y producción se deberían separar para reducir los riesgos de acceso no autorizado o los cambios al sistema operacional.

En su respuesta, la Municipalidad de Diego de Almagro indicó, que el servidor en mención solo es utilizado para operaciones de producción, sin embargo, se evaluará con el comité la posibilidad de implementar un sistema de respaldo que nos permita levantar los servicios en caso de alguna perdida en la conectividad del servidor central.

Referente a este punto, se mantienen las observaciones, pues el servicio indica utilizar el servidor solo para producción, pero debe establecer políticas de respaldo y hacer pruebas de sus restauraciones, por lo que deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir las evidencias que respalden la habilitación de un ambiente de prueba.

12.b) Implementación de medidas contra código malicioso.

De la revisión efectuada a las alertas de seguridad, se evidenció que en el año 2017, y en los meses de marzo y abril de 2021, el servicio fue afectado por el virus ramsonware de extensión .OPTIMUS y .EKING, comprometiendo la información de todas las bases de datos administradas por el municipio de las áreas municipal, salud y educación, desde los sistemas giradores (control de documentos, licencias de conducir, permisos de circulación, patentes comerciales, honorarios, exámenes teóricos) hasta los sistemas financiero-contables proporcionados por CAS Chile e incluidos en el proyecto SIFIM (contabilidad, tesorería, ordenes de ingreso, planificación presupuestaria, conciliaciones, adquisiciones, activo fijo, personal y remuneraciones).

Lo anterior, conllevó a la caída de sus servicios, tiempos de restablecimiento significativos, incidencias en la recuperación de la información (ver apartado 13.b. Copias de seguridad) advirtiendo las siguientes observaciones:

12.b.a) Referente a la infraestructura tecnológica implementada por la entidad

Se verificó que la infraestructura tecnológica de seguridad informática implementada por el municipio, no se condice con los eventos provocados por la acción de software malicioso de mayor grado de peligrosidad y que afectó la integridad de sus servicios, toda vez que el software antivirus utilizado en un total de 17 equipos computacionales, corresponde a la versión que viene instalado por defecto en el sistema operativo Windows (pudiendo ser Microsoft Security Essentials, Windows Defender o Microsoft Defender), y en algunos equipos se ha instalado un antivirus de libre edición (AVG Free, Avira Free o Avast Free), los cuales resultan ser ineficaces para brindar protección a sus sistemas. El listado de los equipos se encuentra en anexo N° 11.

En su respuesta, la entidad comunal indicó, que se encuentra en proceso la habilitación de un cortafuegos (firewall) con el fin de filtrar las conexiones entrantes y salientes de la red municipal y evitar infecciones como las ya ocurridas hasta el momento, así como evaluar la implementación de software antivirus licenciado para tener un monitoreo en tiempo

real de las transacciones realizadas a través de la red y en los equipos con mayor prioridad según lo defina el comité de seguridad.

De acuerdo con lo anterior se debe mantener lo observado, dado que las medidas comprometidas aún no se han concretado, por lo cual el servicio deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir un informe sobre la habilitación del equipo firewall que indica, además de un plan de mejora a su infraestructura tecnológica que incluya la adquisición de un software antivirus.

12.b.b) Sobre sistemas de protección del servidor SIFIM

De la validación efectuada a través del registro fotográfico proporcionado por don [redacted], Jefe del Departamento de Informática del municipio a través de correo electrónico de fecha 23 de septiembre de 2021, se constató que el servidor SIFIM [redacted] no cuenta con un antivirus instalado en su sistema operativo Windows Server 2008 R2 Standard.

Asimismo, se pudo advertir que el servidor SIFIM mantiene el software Malwarebytes antimalware, sin embargo, este último, no brinda protección en tiempo real, así como tampoco es posible la ejecución de análisis programados y que además se detectaron un total de 334 elementos en estado de cuarentena los cuales no han sido atendidos.

Las situaciones descritas en las letras 12.b.a), 12.b.b), incumplen lo exigido en el artículo 26, letra a) del citado decreto N° 83, de 2004, así como también, vulnera lo dispuesto el numeral 10.4.1, de la NCh 27.002 de 2009, dispone que se deberían implementar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto a procedimientos adecuados para concientizar a los usuarios y que el uso de dos o más productos de software que protegen contra código malicioso a través del tratamiento de la información de diversos vendedores puede mejorar la eficiencia de la protección contra el código malicioso.

En este sentido, el numeral 10.4.1, letra d), de la citada norma chilena, señala que la instalación y actualización regular del antivirus para detección y reparación de software que exploren los computadores y los soportes de forma rutinaria o como un control preventivo, cuyas verificaciones deberían incluir; 1) la comprobación de archivos en medios electrónicos y ópticos, y archivos recibidos a través de redes, para verificar la existencia de código malicioso, antes de su uso y 2) la comprobación para buscar software malicioso, antes de usarlo, de todo archivo adjunto a un correo electrónico o de toda descarga. Esta comprobación que se hará en distintos lugares, por ejemplo, en los servidores de correo, en los computadores terminales o a la entrada en la red de la organización.

En su respuesta, el servicio señaló, que se encuentra en proceso la habilitación de un cortafuegos (firewall) con el fin de filtrar las conexiones entrantes y salientes de la red municipal y evitar infecciones como las ya ocurridas hasta el momento, así como evaluar la implementación de software

antivirus licenciado para tener un monitoreo en tiempo real de las transacciones realizadas a través de la red y en los equipos con mayor prioridad según lo defina el comité de seguridad. Indica, además, se evaluará con el comité alguna otra mejora para la implementación de seguridad en el servidor, sin afectar los tiempos de respuesta para los procesos que se ha configurado.

De acuerdo con lo anterior se mantiene la observación, pues el servicio indica medidas que aún no se han concretado, por lo cual deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir un informe sobre la habilitación del equipo firewall que indica, además de un plan de mejora a su infraestructura tecnológica que incluya la adquisición de un software antivirus para el servidor.

12.c) Ausencia de un plan de continuidad.

Se observó, que la entidad no ha implementado un plan de continuidad que establezca los procedimientos para la recuperación ante los potenciales ataques de código malicioso, que incluya todos los datos y software necesarios de respaldo, situación que vulnera lo contenido en el numeral 10.4.1, letra f), de la NCh 27.002 de 2009, que dispone que se deberían definir procedimientos y responsabilidades de gestión para la protección de los sistemas contra código malicioso, la capacitación para su uso, la información de los ataques de los virus y la recuperación de éstos.

En su respuesta, la entidad municipal señaló que se evaluará con el comité la posibilidad de implementar un sistema de respaldo que permita dar continuidad al servicio mientras se repara la incidencia en el servidor central.

Referente a este punto, se mantiene lo observado, debido a que las gestiones anunciadas, no se han materializado, por lo cual el servicio deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir un plan de continuidad que establezca los procedimientos para la recuperación ante los potenciales ataques de código malicioso, que incluya todos los datos y software necesarios de respaldo.

12.d) Equipos con Microsoft Windows sin actualizar.

Se evidenció que un total de 5 equipos computacionales reportan falta de actualizaciones del sistema operativo Windows, las que se detallan en la siguiente tabla:

Tabla N° 1: Detalle de equipos desactualizados.

N°	Serie	Marca y Modelo	Nombre Equipo	Tipo	Sistema Operativo
[redacted]	[redacted]	Lenovo Thinkcentre E73Z	[redacted]	[redacted]	WIN 7 Pro
[redacted]	[redacted]	HP 24-B208LA AIO	[redacted]	[redacted]	WIN 10 Home SL(*)

N°	Serie	Marca y Modelo	Nombre Equipo	Tipo	Sistema Operativo
[redacted]	[redacted]	HP Probook 440 G1	[redacted]	[redacted]	WIN 7 PRO
		HP 530 Notebook PC			WIN 7 PRO
		Lenovo Thinkcentre E73Z			WIN 7 PRO

Fuente: Elaboración propia en base a los antecedentes proporcionados por don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro, mediante correo electrónico de fecha 24 de septiembre de 2021.
(*) Falta actualización de características

Lo anteriormente expuesto, no se ajustan a lo contenido en el numeral 12.5.3 de la NCh ISO 27.002 de 2009, la cual señala que un proceso de gestión de actualización de software debería ser puesto en práctica para asegurar que los parches más actualizados aprobados y actualizaciones de aplicación son instalados para todo el software autorizado.

En su respuesta, el servicio indicó que los equipos listados no cumplen las condiciones de hardware para realizar la actualización de sistema, prontos a ser dados de baja o mejorar mediante la implementación de hardware más actualizado y que permita extender su vida útil.

Referente a este punto, se debe mantener lo observado, pues la entidad da cuenta de acciones futuras que se podrían llevar a cabo para su subsanación, pero no anuncia medidas concretas. A su vez, no se adjunta respaldo de que los computadores observados no cumplen con las condiciones de hardware para realizar la actualización de su sistema, por lo que la entidad deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir un informe con el estado de actualización de estos equipos, el cual incluya fundamentos técnicos de que los equipos no cumplen con las condiciones de hardware para recibir actualizaciones y un plan de renovación de equipos computacionales que incluya responsables y plazos concretos para su ejecución.

13. Integridad y disponibilidad de la información.

Como cuestión previa, es del caso indicar que la entidad señaló que las copias de seguridad son proporcionadas por el Grupo GTD (ex-Intesis), con administración en la ciudad de Santiago, las cuales se encuentran en convenio junto con la implementación del proyecto SIFIM a través de la SUBDERE aproximadamente desde el año 2012.

Agrega que, en la última afectación por el virus ramsonware, en abril de 2021, la empresa no disponía de las últimas copias de seguridad, a consecuencia de una falla de conectividad hasta ese momento desconocida, entre el servidor SIFIM del municipio que contiene la información a respaldar y el equipo firewall Fortinet del grupo GTD, que realiza respaldos

automáticos en red, a través de técnicas de log shipping.[7]. Incidencia que fue resuelta por copias de seguridad locales que el Municipio mantenía y que lograron ser restauradas.

En consecuencia, la entidad manifestó que solo disponen en la actualidad de las copias de seguridad locales, las que son creadas mediante programación automática en el servidor, rescatadas por el Jefe de Informática del municipio y almacenadas en un disco duro externo y en un computador auxiliar que permanecen en el Departamento de Informática.

Conforme a los antecedentes aportados por el servicio, y de las validaciones efectuadas a las copias de seguridad de la base de datos de CAS Chile, se realizaron las siguientes observaciones:

13.a) Información no proporcionada.

La entidad no proporcionó a este organismo fiscalizador los contratos y/o convenios sobre servicios externalizados, específicamente el contrato actual de SIFIM, solicitado mediante correo electrónico de fecha 13 de julio de 2021, reiterado por oficio N° E128067, de 2021 y por correo electrónico de fecha 23 de agosto, por tanto, no fue posible tomar conocimiento de las responsabilidades que deben ser atribuidas al municipio o a la empresa GTD sobre los procesos de copias de seguridad y restauración de sus sistemas.

Lo anterior, denota la falta de conocimiento que la municipalidad mantiene sobre estos contratos y/o convenios y sus cláusulas, pues si en el origen, la labor de mantener copias de seguridad pertenecía a la empresa, se podría estar pagando por un servicio no realizado, sin perjuicio que el propio municipio mantenga un procedimiento informal de creación de copias de seguridad de sus sistemas.

Lo expuesto no se condice con lo establecido con lo establecido en el artículo 17 de la antes citada resolución N° 10, de 2021, el cual señala, en lo que interesa, que la entidad o servicio auditado dispondrá que quienes se relacionen con las materias auditadas cooperen en el desarrollo de la auditoría; proporcionará los accesos a las bases de datos y antecedentes requeridos en los plazos definidos.

A su vez, lo descrito constituye una vulneración a los principios de responsabilidad, eficiencia, eficacia, contenidos en los artículos 3° y 11 de la mencionada ley N° 18.575, según los cuales el control se extenderá tanto a la eficiencia y eficacia en el cumplimiento de los fines y objetivos establecidos, como a la legalidad y oportunidad de las actuaciones, añadiendo su artículo 5° que las autoridades y funcionarios deberán velar por la eficiente e idónea

[7] Log Shipping se refiere al proceso de respaldar automáticamente la base de datos y el log de transacciones, restaurándolos en un servidor de respaldo. Esto mantiene a los dos equipos en sincronía en caso de que el servidor de producción tenga alguna falla.

administración de los medios públicos y por el debido cumplimiento de la función pública.

Además, se advierte una transgresión a lo prescrito en el artículo 53 de la referida ley N° 18.575, que exige el empleo de medios idóneos de diagnóstico, decisión y control, para concretar, dentro del orden jurídico, una gestión en plena concordancia con los aludidos principios de eficiencia y eficacia, lo que no ha sucedido en la especie.

Con todo, es del caso recordar que los principios antes aludidos obedecen al logro de metas y al uso óptimo de los recursos estatales, respectivamente, con el propósito de alcanzar los objetivos públicos con el menor costo para la Administración (aplica criterio contenido, entre otros, en los dictámenes N^{os} 25.737, de 1995; 46.618, de 2000; 7.347, de 2013, y 88.553, de 2015, de la Contraloría General).

En su respuesta, la entidad municipal señaló que se elevaron los requerimientos para dar con las copias de los convenios, pero sin resultados positivos a la fecha, se continuarán los esfuerzos por disponer de esta documentación, a fin de esclarecer las responsabilidades correspondientes a cada entidad participante en dicho convenio.

Según lo anterior, se mantienen las observaciones, dado que las gestiones anunciadas por el servicio, tendientes a subsanar las situaciones detectadas corresponden a acciones futuras no materializadas a la fecha, por lo cual la entidad deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir el convenio actual de SIFIM y una aclaración de las responsabilidades que deben ser atribuidas al municipio o a la empresa GTD sobre los procesos de copias de seguridad y restauración de sus sistemas.

13.b) Copias de seguridad.

Se verificó que el municipio no dispone de una política de respaldo formal de sus sistemas la cual contenga al menos, los procedimientos técnicos de copias de seguridad y restauración, estrategias ante contingencias, planificación de ensayos de restauración y responsables, vulnerando el numeral 10.5 de la NCh ISO 27.002 de 2009, la cual señala que para mantener la integridad y disponibilidad de la información y de las instalaciones de procesamiento de la información, se deberían establecer procedimientos de rutina para implementar una política y estrategia acordada de respaldo haciendo copias de respaldo de datos y ensayando sus tiempos de restauración.

Agrega en el numeral 10.5.1 de la mencionada norma chilena, que se deberían hacer regularmente copias de seguridad de la información y del software y probarse regularmente acorde con la política de respaldo.

En su respuesta, el servicio señaló que se incluirán en las políticas de seguridad un apartado para el servidor y sus procedimientos técnicos de copias de seguridad y restauración, entre otras.

De acuerdo con su respuesta, se mantiene la observación, debido a que las gestiones anunciadas, aún no se han materializado, por lo cual la entidad deberá remitir, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, la política de respaldo formal de sus sistemas la cual contenga al menos, los procedimientos técnicos de copias de seguridad y restauración, estrategias ante contingencias, planificación de ensayos de restauración y responsables.

13.c) Referente al proceso de restauración de base de datos

Se constató que la entidad no realiza ensayos de restauración de la base de datos de su sistema de información en el servidor SIFIM y que, además, se encuentre documentada, toda vez que no se han separado los ambientes de producción y prueba de sus sistemas. (ver numeral 12.a) Ambientes de producción y prueba), vulnerando lo establecido en el numeral 10.5.1, letra g) de la NCh ISO 27.002 de 2009, la cual señala que los procedimientos de restauración se deberían comprobar regularmente para asegurar que son eficaces y que pueden ser utilizados dentro del tiempo asignado en los procedimientos operacionales para la recuperación.

En su respuesta, la entidad municipal señaló que se registrarán los eventos de seguridad de la información y funcionamiento del servidor, quedando establecido el procedimiento en las políticas de seguridad.

De acuerdo con lo anterior se debe mantener lo observado, dado que las medidas comprometidas aún no se han concretado, por lo cual el servicio deberá remitir, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, la política de respaldo formal de sus sistemas la cual contenga al menos, los procedimientos técnicos de copias de seguridad y restauración, estrategias ante contingencias, planificación de ensayos de restauración y responsables. Además de adjuntar las capturas de pantalla de la restauración a la última copia de seguridad generada.

13.d) Registro de fallas (logs).

Se evidenció que la entidad no posee registros de los eventos de seguridad de la información y sus fallas, con el fin de detectar actividades no autorizadas en el servidor SIFIM y sus sistemas y que tampoco ha realizado seguimiento a estas fallas, lo cual no se aviene a lo contemplado en el numeral 10.10 de la Nch 27.002 de 2009, el que dispone que se deberían supervisar los sistemas y registrarse los eventos de seguridad de la información. Registros del operador y de fallas deberían ser utilizados para asegurar que los problemas en los sistemas de información son identificados.

Agrega el numeral 10.10.5 de referida norma chilena de 2009 que expone que las fallas deberían ser registradas, analizadas y tomadas las acciones apropiadas.

En su respuesta, el municipio señaló que se registrarán los eventos de seguridad de la información y funcionamiento del servidor, quedando establecido el procedimiento en las políticas de seguridad.

Referente a este punto, las gestiones anunciadas por el servicio corresponden a eventos que no se han materializado, por lo cual se debe mantener la observación, debido la entidad, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, remitir el procedimiento de registro de fallas debidamente formalizado.

13.e) Vulnerabilidades de los sistemas informáticos.

Del escaneo de puertos realizado al servidor SIFIM, que soporta al sistema de gestión municipal, utilizando la herramienta de exploración NMAP, se detectaron vulnerabilidades que aumentan el riesgo de sufrir ataques del tipo denegación de servicio, intercepción de tráfico en la red y acceso a información sensible, cuyo detalle se presenta a continuación:

Tabla N° 2: Detalle de debilidades detectadas.

HOST	Descripción	Comando	Vulnerabilidad	Código de Vulnerabilidad
[redacted]				

Fuente: Elaboración propia de acuerdo con los resultados obtenidos del escaneo de NMAP efectuado a través de videollamada realizada a través de la plataforma TEAMS, el día miércoles 26 de agosto de 2021.

La situación descrita, no se condice con lo establecido en el numeral 12.6, de la norma chilena NCh-ISO 27.002, de 2009, el cual indica que la gestión de vulnerabilidades técnicas se debería implementar como una manera eficaz, sistemática, y repetible con ejecución de mediciones para confirmar su eficacia. Estas consideraciones deberían incluir los sistemas operativos, y cualquier otra aplicación en uso.

En su respuesta, el servicio señaló que las vulneraciones descritas en los puertos del servidor serán resueltas una vez se disponga de la configuración final del firewall por parte del proveedor de enlaces.

Según lo anterior, se mantienen las observaciones, dado que las gestiones anunciadas por el servicio, tendientes a subsanar las situaciones detectadas corresponden a acciones futuras no

materializadas a la fecha, por lo cual la entidad deberá, en un plazo no superior a 60 días hábiles contados a partir de la recepción del presente informe, dar cuenta de la atención de estas vulnerabilidades.

CONCLUSIONES

Atendida las consideraciones expuestas durante el desarrollo del presente trabajo, y dado que las medidas anunciadas por la Municipalidad de Diego de Almagro respecto las situaciones planteadas en el Preinforme de Observaciones N° 1.022, de 2021, son de aplicación futura, esta Contraloría Regional, ha estimado pertinente mantenerlas en todas sus partes, debiendo esa entidad comunal adoptar las medidas con el objeto de dar estricto cumplimiento a las normas legales y reglamentarias que las rigen, entre las cuales se estima necesario considerar, a lo menos, las siguientes:

1. En lo relacionado con las observaciones contenidas en los numerales 1.1 Sobre manuales de procedimientos sin formalizar y 1.2 Sobre manual de procedimiento desactualizado, (MC), la Municipalidad de Diego de Almagro, deberá remitir el manual de procedimientos de informática y el manual de procedimiento para el alta, baja y cambio de usuarios que trabajan con los Sistemas de Información Financiera Municipal, SIFIM, y Mercado Público debidamente actualizado y formalizado, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

2. Respecto a las observaciones contenidas en el numeral 1.3 Sobre falta de cumplimiento a las disposiciones contenidas en manuales de procedimiento, (MC), la entidad comunal, deberá emitir un informe con las gestiones realizadas tendientes a subsanar las observaciones descritas en el Anexo N° 1, adjuntando respaldo de las difusiones al personal a través de correos electrónicos, registro de capacitaciones y actas de entrega de documentación, además de abordar las responsabilidades que le competen al Departamento de Informática sobre la materia observada, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

3. Referente a los manifestado en el numeral 2.1 Sobre Ausencia de un inventario de activos de tecnologías de la información, (MC), el servicio, deberá remitir el inventario de los activos computacionales -hardware y software-, debidamente registrados con códigos de inventario asignados por la institución, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

4. En lo que dice relación a lo observado en numeral 3.a) Falta de designación del Encargado de Seguridad de la Información, (MC), la entidad municipal, deberá remitir la designación formal del Encargado de Seguridad de la Información, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

5. Sobre las observaciones formuladas en el numeral 3.b) Inexistencia de un Comité de Seguridad de la Información, (MC), el servicio, deberá remitir la designación formal del Comité de Seguridad de la Información, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

6. En lo relacionado con las observaciones contenidas en los numerales 4.a) Ausencia de política de seguridad de la información y 4.b) Contenido de la política de seguridad de la información, (MC), la Municipalidad de Diego de Almagro, deberá remitir la política de seguridad de la información, la cual tendrá que ser acreditada en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

7. Respecto a las observaciones contenidas en el numeral 4.c.a) Referente al proceso de adquisición e instalación de equipos, (MC), el municipio, deberá remitir un documento oficial que señale las responsabilidades sobre la adquisición, registro del inventario, instalación, habilitación, configuración e implementación de recursos informáticos, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

8. En lo que dice relación al numeral 4.c.b) Respecto del uso del correo institucional, (MC), el servicio, deberá remitir los respaldos de las difusiones y/o capacitaciones realizadas con respecto de los riesgos asociados al uso del correo electrónico institucional, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

9. Conforme a las observación descrita en el numeral 4.d) Información no proporcionada, (MC), el servicio, deberá remitir las últimas 5 solicitudes de alta/baja y/o modificación de usuarios SIFIM debidamente regularizadas o presentar un documento oficializado que actualice lo descrito en el manual de procedimiento para el alta, baja y cambio de usuarios que trabajan con los Sistemas de Información Financiera Municipal, SIFIM, y Mercado Público, autorizado mediante acta de acuerdo N° 79, del Concejo Municipal, de fecha 8 de mayo de 2012, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

10. Sobre lo advertido en el numeral 5.a) Ausencia de evaluación de riesgos, (MC), la Municipalidad, deberá remitir el informe de evaluación de riesgos, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

11. En consideración de lo expuesto en el numeral 6.a) Clasificación y control de bienes, (MC), la entidad comunal, deberá remitir el catastro de equipos computacionales del departamento de Informática actualizado y con las correcciones necesarias para subsanar la observación, lo cual

tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

12. Conforme al numeral 6.b) Ausencia de un catastro de software en inventario de activos de tecnologías de la información, (MC), el servicio, deberá remitir el catastro de software que incluya las licencias adquiridas y las instaladas, indicando el usuario que le fue asignado, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

13. Con respecto a lo observado en el numeral 6.c) Inconsistencias en el catastro de activos de tecnologías de la información, (MC), la entidad, deberá remitir el catastro de equipos computacionales con todas las correcciones necesarias para subsanar la observación, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

14. En lo relacionado con las observaciones contenidas en el numeral 7.a) Sobre configuración de cuentas de usuarios en Windows con privilegios de administrador, (MC), la Municipalidad de Diego de Almagro, deberá remitir la aclaración por los cuatro equipos computacionales asignados a los usuarios [redacted] los cuales no tienen instalado el sistema Cas Chile y sin embargo mantienen cuenta con privilegios administrativos, y además, remitir un documento del proveedor CAS Chile que certifique que las cuentas de usuario Windows deben ser configuradas con privilegios de administrador para el manejo de sus sistemas, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

15. Sobre lo advertido en el numeral 7.b) Sobre utilización de cuentas de usuarios genéricas en Windows, (MC), el servicio, deberá dar cuenta de la regularización de los 17 casos observados, a través de una captura de pantalla de la cuenta de usuario donde se identifique el funcionario que tiene asignado el equipamiento, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

16. En consideración de lo expuesto en en el numeral 7.c) Sobre irregularidades en las cuentas de usuarios en sistema SIFIM, (MC), el municipio, deberá remitir una nueva nómina en formato Excel (xls o xlsx) con las cuentas de usuario del Sistema SIFIM, en donde se evidencie las modificaciones y/o eliminaciones, además de un certificado firmado que respalde el archivo digital, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

17. Con respecto a lo observado en el numeral 7.d) Respecto de la configuración de contraseñas (MC), la entidad, deberá remitir las gestiones realizadas con el proveedor de sistemas para modificar la

extensión y complejidad de las contraseñas para dar cumplimiento de la normativa, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

18. Conforme al numeral 7.e) Sobre período de actualización de contraseñas, (MC), la entidad comunal, deberá definir el procedimiento para cambiar los identificadores a intervalos regulares y comunicar las adecuaciones en la plataforma tecnológica, indicando el usuario que le fue asignado, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

19. De acuerdo con lo avenido en el numeral 7.f) Equipos computacionales con acceso liberado, (MC), el servicio, deberá remitir las capturas de pantalla que den cuenta de la identificación del usuario y el bloqueo de redes sociales, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

20. En lo relacionado a los numerales 9.a) Ausencia de bitácoras de acceso a sala de servidores y 9.i) Sobre implementación de bitácoras de fallas en sala de servidores (MC), la entidad municipal, deberá remitir evidencia de la puesta en marcha de una bitácora física, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

21. Referente a las observaciones descritas en los numerales 9.b) Inexistencia de puerta de cortafuego, 9.c) Inexistencia de sistemas de emergencia en sala de servidores, 9.d) Falta de sistema de iluminación de emergencia, 9.g) Sobre seguridad implementada en sala de servidores, 9.h) Sobre instalaciones eléctricas en sala de servidores, (MC), la Municipalidad de Diego de Almagro, deberá remitir un plan de mejora para la sala de servidores que incluya la instalación, mejora o modificación de los elementos observados, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

22. Seguidamente, en lo observado en el numeral 9.e) Sobre señalética en sala de servidores, (MC), la entidad edilicia, deberá remitir las fotografías que den cuenta de la habilitación de carteles en lugares visibles que establezcan las prohibiciones de fumar, consumir alimentos y/o bebidas, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

23. Luego, en lo avenido en el numeral 9.f) Referente a equipo de ventilación en sala de servidores, (MC), el servicio, deberá remitir el estado de habilitación y funcionamiento del equipo de aire acondicionado para subsanar la observación, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

24. Con respecto a lo observado en el numeral 10.a) Procedimientos de destrucción de información, (MC), la entidad, deberá remitir los procedimientos formales relacionados con los procesos de destrucción de información de los equipos en desuso, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

25. Sobre lo advertido en el numeral 10.b) Controles criptográficos, (MC), el servicio, deberá definir y comunicar formalmente cuál es la información sensible afecta a ser cifrada en la base de datos del sistema SIFIM, o en su defecto, comunicar el respaldo de las gestiones con el proveedor de software para cifrar los datos contenidos en las tablas de datos, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

26. Conforme al numeral 11.a) Utilización de licencias de Microsoft Office no autorizadas, (MC), la entidad, deberá remitir el contrato con la empresa Microsoft que acredite la disponibilidad de las descargas para realizar el downgrade a los equipos informáticos del Municipio, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

27. Según lo observado en el numeral 11.b) Compra de licencias de software Microsoft Office no instaladas, (MC), la Municipalidad de Diego de Almagro, deberá remitir un plan de renovación de equipos computacionales que permitan la instalación del software adquirido, que incluya responsables y plazos concretos para su ejecución, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

28. En cuanto a la observación del numeral 11.c) Utilización de otros softwares no autorizados, (MC), la entidad, deberá remitir las capturas de pantalla del panel de control que evidencie la eliminación del software, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

29. Referente a lo observado en el numeral 12.a) Ambientes de producción y prueba, (MC), la entidad, deberá remitir las evidencias que respalden la habilitación de un ambiente de prueba en el servidor SIFIM, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

30. En cuanto a lo descrito en los numerales 12.b.a) Referente a la infraestructura tecnológica implementada por la entidad y 12.b.b) Sobre sistemas de protección del servidor SIFIM, (MC), el ente edilicio, deberá remitir un informe sobre la habilitación del equipo firewall que indica, además de un plan de mejora a su infraestructura tecnológica que incluya la adquisición de un software antivirus, lo cual tendrá que ser acreditado en el Sistema

de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

31. Sobre lo advertido en el numeral 12.c) Ausencia de un plan de continuidad, (MC), el servicio, deberá remitir un plan de continuidad que establezca los procedimientos para la recuperación ante los potenciales ataques de código malicioso, que incluya todos los datos y software necesarios de respaldo, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

32. Con respecto a lo observado en el numeral 12.d) Equipos con Microsoft Windows sin actualizar, (MC), la entidad comunal, deberá remitir un informe con el estado de actualización de estos equipos, el cual incluya fundamentos técnicos de que los equipos no cumplen con las condiciones de hardware para recibir actualizaciones y un plan de renovación de equipos computacionales que incluya responsables y plazos concretos para su ejecución, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

33. Sobre las observaciones formuladas en el numeral 13.a) Información no proporcionada, (MC), el servicio, deberá remitir el convenio actual de SIFIM y una aclaración de las responsabilidades que deben ser atribuidas al municipio o a la empresa GTD sobre los procesos de copias de seguridad y restauración de sus sistemas, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

34. Seguidamente, en lo observado en los numerales 13.b) Copias de seguridad y 13.c) Referente al proceso de restauración de base de datos, (MC), la entidad edilicia, deberá remitir la política de respaldo formal de sus sistemas la cual contenga al menos, los procedimientos técnicos de copias de seguridad y restauración, estrategias ante contingencias, planificación de ensayos de restauración y responsables. Además de adjuntar, para el caso del numeral 13.c), las capturas de pantalla de la restauración a la última copia de seguridad generada, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

35. Luego, en lo avenido en el numeral 13.d) Registro de fallas (logs), (MC), el servicio, deberá remitir el procedimiento de registro de fallas debidamente formalizado, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

36. Para lo advertido en el numeral 13.e) Vulnerabilidades de los sistemas informáticos, (MC), el servicio, deberá dar cuenta de la atención de estas vulnerabilidades, lo cual tendrá que ser acreditado en el

Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.

Finalmente, para aquellas observaciones que se mantienen, que fueron catalogadas como AC y/o C, identificadas en el "Informe de Estado de Observaciones", de acuerdo al formato adjunto en el Anexo N° 12, las medidas que al efecto implemente el servicio, deberán acreditarse y documentarse en el Sistema de Seguimiento y Apoyo CGR, que esta Entidad de Control puso a disposición de las entidades públicas, según lo dispuesto en el oficio N° 14.100, de 6 de junio de 2018, de este origen en un plazo de 60 días hábiles, o aquel menor que se haya indicado, contado desde la recepción del presente informe.

Respecto de aquellas observaciones que se mantienen y que fueron categorizadas como MC y/o LC en el citado "Informe de Estado de Observaciones", el cumplimiento de las acciones correctivas requeridas deberá ser informado por las unidades responsables al Encargado de Control/Auditor Interno, a través del Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, quien a su vez deberá acreditar y validar en los siguientes 30 días hábiles la información cargada en la ya mencionada plataforma, de conformidad a lo establecido en el aludido oficio N° 14.100, de 2018.

Remítase al Alcalde, Director de Control Interno y al Secretario Municipal, todos de la Municipalidad de Diego de Almagro.

Saluda atentamente a Ud.,

Firmado electrónicamente por:	
Nombre:	ELIZABETH CARIAGA ARRIAGADA
Cargo:	Jefa de Unidad de Control Externo
Fecha:	25/04/2022

Anexo N°1: Cláusulas del Manual de procedimiento de Informática que no se han dado cumplimiento.

N°	Sección	Texto del documento	Observación
1	Políticas operativas para el uso de estaciones de trabajo y periféricos letra j) Sobre el uso del servicio de internet, letra e).	No copiar o "Piratear" sistemas programados, a menos que este sea de dominio público (Shareware, Freeware); es ilegal y está estrictamente prohibido, ya que puede significar para el municipio sanciones legales.	Se constataron programas no licenciados (Acápite II: Examen de la Materia Auditada, Numeral 11).
2	Políticas operativas para el uso de estaciones de trabajo y periféricos letra n)	El usuario no deberá instalar software no autorizado, (ni siquiera un simple protector de pantalla), ya que puede infectar el equipo y redes. Esto puede ocasionar pérdidas importantes de información, así como también consecuencias irremediables.	Existen equipos que mantienen software no autorizado (Acápite II: Examen de la Materia Auditada, Numeral 11), además de equipos que mantienen un protector de pantalla distinto al institucional.
3	Adquisición de equipos.	Es responsabilidad del Departamento de Informática la instalación de equipos computacionales, como también la realización de las pruebas técnicas respectivas.	No todos los equipos que se adquieren son instalados por el Departamento de Informática.
4	Sobre el uso del servicio de internet, letra b)	El Departamento de Informática estará facultada de forma periódica para revisar los archivos de registro (logs) del uso de Internet y Servidores.	Se constató que no existe revisión de logs en el servidor (Acápite II: Examen de la Materia Auditada, Numeral 13.d).
5	Procedimiento uso del correo electrónico, letras a), b), c), d), e), f) y g)	En síntesis: Creación de cuentas, propiedad de la casilla, soporte informático, cadenas de correo, alerta de mensajería, listas de distribución, uso de correos masivos.	Se advirtió que la entidad no ha realizado difusión de la información a través de correo electrónico y/o capacitaciones a los funcionarios sobre el riesgo asociado al uso del correo electrónico

CONTRALORIA REGIONAL CONTRALOR REGIONAL ATACAMA

Anexo N°1: Cláusulas del Manual de procedimiento de Informática que no se han dado cumplimiento (continuación)

N°	Sección	Texto del documento	Observación
6	Sobre el uso del servicio de internet, letra c)	El Departamento de Informática estará facultada para filtrar páginas Web, controlando el contenido de las páginas durante el proceso de navegación.	No se ha establecido un bloqueo de redes sociales. (Acápite II: Examen de la Materia Auditada, Numeral 7, letra f).
7	Autentificación de usuarios y datos, letra a)	La autenticación de usuarios consiste en verificar que el usuario es quién realmente dice ser. Lo anterior, se logra a través de mecanismos de autentificación como la clave de acceso y password de cada usuario.	la municipalidad utiliza cuentas de usuario de Windows genéricas (Acápite II: Examen de la Materia Auditada, Numeral 7, letra b).
8	Protección del servidor, letra b)	Un conjunto de respaldos de la información de los servidores se deberá trasladar a otro lugar seguro (caja fuerte municipal).	Se constató que estos respaldos se almacenan en el Departamento de Informática y no en el lugar indicado en el manual. (Acápite II: Examen de la Materia Auditada, Numeral 9, letra j).
9	Protección del servidor, letra d)	Se debe Llevar una estadística de los problemas e incidencias para ajustar lo mejor posible el mantenimiento preventivo, esta bitácora incluirá todos los servicios de comunicaciones.	Se evidenció que el Departamento de Informática no mantiene una bitácora de fallas (Acápite II: Examen de la Materia Auditada, Numeral 9, letra i).

Fuente: Elaboración propia basada en las validaciones efectuadas y a los antecedentes proporcionados por don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro, mediante correo electrónico de fecha 23 de septiembre de 2021.

Anexo N°2: Catastro de activos de tecnologías de la información incompleto y desactualizado.

Serie	Marca y Modelo	Tipo de equipo	Nombre Equipo	Funcionario Asignado	Estado equipo	
					Inventario	Real
[redacted]	Genérico (Sentey Gabinete) Negro	PC	[redacted]	[redacted]	En uso	Malo
	HP Compaq Pro 4300 AIO PC	PC			En uso	Baja
	Genérico Color negro con verde Pentium 4 1,80 GHZ	PC			En uso	Malo

Fuente: Elaboración propia en base a las validaciones realizadas y a la información proporcionada por don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro a través de correo electrónico de fecha 13 de agosto de 2021.
S/I = Sin información.

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

Anexo N° 3: Equipos computacionales asignados a funcionarios distintos de la muestra.

Serie	Marca y Modelo	Tipo	Nombre Equipo	Muestra			Validación		
				Funcionario	Departamento	Área	Funcionario	Departamento	Área
[redacted]	HP Pro 3400 Series MT	PC	[redacted]						
	HP Probook 440 G1	NTB							
	Genérico (Sentey Gabinete) negro	PC							
	Genérico (Sentey Gabinete) negro	PC							
	HP Pro 3420 AIO PC	PC							
	HP 530 Notebook PC	NTB							

Fuente: Elaboración propia realizado en base a las validaciones efectuadas y a los antecedentes proporcionados por don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro a través de correo electrónico de fecha 23 de septiembre de 2021.

Anexo N° 4: Usuarios con cuentas de acceso de Windows con privilegios de Administrador.

N°	Usuario	Nombre equipo	Serie	Departamento	Área	Cuenta de acceso
[redacted]				Dirección de Administración y Finanzas	[redacted]	
				Dirección de Administración y Finanzas		
				Dirección de Administración y Finanzas		
				Dirección de Administración y Finanzas		
				Control Interno		
				Dirección de Administración y Finanzas		
				Dirección de Administración y Finanzas		
				Dirección de Administración y Finanzas		
				Dirección de Administración y Finanzas		

Anexo N° 4: Usuarios con cuentas de acceso de Windows con privilegios de Administrador. (continuación)

N°	Usuario	Nombre equipo	Serie	Departamento	Área	Cuenta de acceso
[redacted]				Dirección de Administración y Finanzas		
				Dirección de Administración y Finanzas		
				Secretaría Municipal		
				Secretaría Municipal		
				Dirección Desarrollo Comunitario		
				Dirección de Administración y Finanzas		
				Secretaría Municipal		
				Control Interno		

Fuente: Elaboración propia realizado en base a las validaciones efectuadas y a los antecedentes proporcionados por don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro a través de correo electrónico de fecha 23 de septiembre de 2021.

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

Anexo N° 5: Sobre utilización de cuentas de usuarios genéricos en Windows.

N°	Usuario	Nombre Equipo	Serie	Departamento	Área	Cuenta De Acceso
[redacted]				Dirección de Administración y Finanzas	[redacted]	
				Dirección de Administración y Finanzas		
				Dirección de Administración y Finanzas		
				Dirección de Administración y Finanzas		
				Control Interno		
				Dirección de Administración y Finanzas		
				Dirección de Administración y Finanzas		
				Dirección de Administración y Finanzas		
				Dirección de Administración y Finanzas		

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

Anexo N° 5: Sobre utilización de cuentas de usuarios genéricos en Windows. (continuación)

N°	Usuario	Nombre Equipo	Serie	Departamento	Área	Cuenta de Acceso
[redacted]				Dirección de Administración y Finanzas	[redacted]	
				Dirección de Administración y Finanzas		
				Secretaría Municipal		
				Secretaría Municipal		
				Dirección de Desarrollo Comunitario		
				Dirección de Administración y Finanzas		
				Secretaría Municipal		
				Control Interno		

Fuente: Elaboración propia realizado en base a las validaciones efectuadas y a los antecedentes proporcionados por don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro a través de correo electrónico de fecha 23 de septiembre de 2021.

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

Anexo N° 6: Análisis de las cuentas de usuario de SIFIM con identificadores genéricos

Nº	ID de Usuario	Nombre del Responsable	Código Sistema	Sistema	Plataforma
[redacted]					

Anexo N° 6: Análisis de las cuentas de usuario de SIFIM con identificadores genéricos (continuación)

Nº	ID de Usuario	Nombre del Responsable	Código Sistema	Sistema	Plataforma
[redacted]					

Anexo N° 6: Análisis de las cuentas de usuario de SIFIM con identificadores genéricos (continuación)

Nº	ID de Usuario	Nombre del Responsable	Código Sistema	Sistema	Plataforma
[redacted]					

Fuente: Elaboración propia realizado en base a las validaciones efectuadas y a los antecedentes proporcionados por don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro a través de correo electrónico de fecha 23 de septiembre de 2021.

Anexo N° 6: Análisis de las cuentas de usuario de SIFIM con identificadores asignados a un responsable genérico (continuación)

Nº	ID de Usuario	RUN	Nombre del Responsable	Código Sistema	Sistema	Plataforma
[redacted]						

Anexo N° 6: Análisis de las cuentas de usuario de SIFIM con identificadores asignados a un responsable genérico (continuación)

Nº	ID de Usuario	RUN	Nombre del Responsable	Código Sistema	Sistema	Plataforma
[redacted]						

Fuente: Elaboración propia realizado en base a las validaciones efectuadas y a los antecedentes proporcionados por don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro a través de correo electrónico de fecha 23 de septiembre de 2021.

ANEXO N° 6: Análisis de las cuentas de usuario de SIFIM con identificadores asignados a un responsable distinto (Continuación)

Nº	ID de Usuario	Rut	Nombre del Responsable	Código Sistema	Sistema	Plataforma
[redacted]						

Fuente: Elaboración propia realizado en base a las validaciones efectuadas y a los antecedentes proporcionados por don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro a través de correo electrónico de fecha 23 de septiembre de 2021.

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

Anexo N° 7: Usuarios con acceso liberado de Internet.

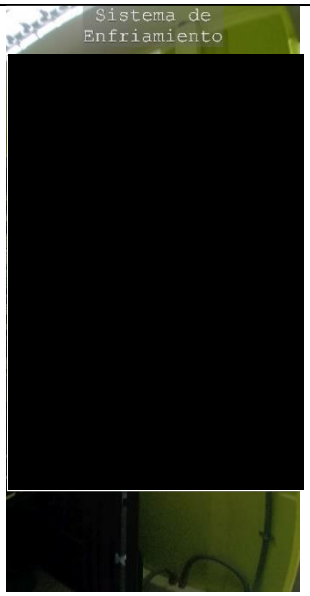
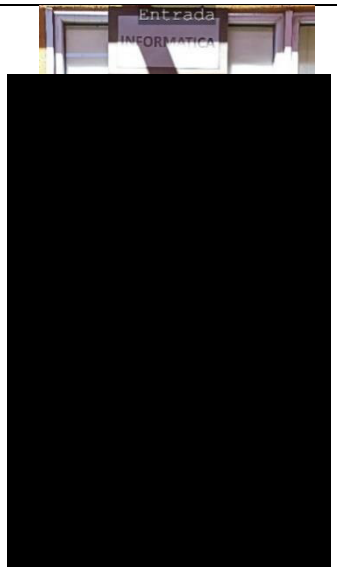
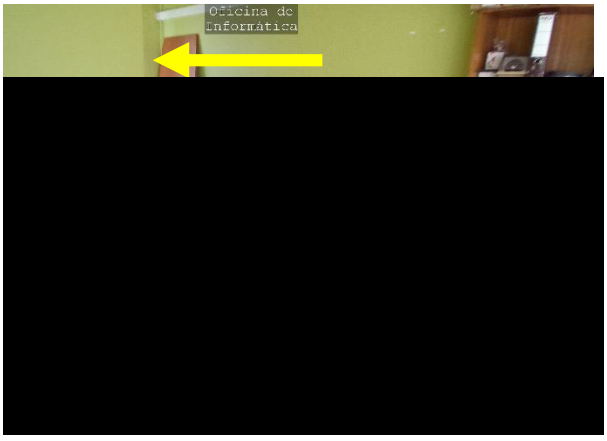
N°	Usuario	Función Efectiva	Nombre Equipo	Serie	Departamento	Área
[redacted]						

Anexo N° 7: Usuarios con acceso liberado de Internet. (continuación)

N°	Usuario	Función Efectiva	Nombre Equipo	Serie	Departamento	Área
[redacted]						

Fuente: Elaboración propia realizado en base a las validaciones efectuadas y a los antecedentes proporcionados por don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro a través de correo electrónico de fecha 23 de septiembre de 2021.

Anexo N° 8: Seguridad Física del Área de Comunicaciones.

	
Fotografía N°1: Puerta de acceso sala de servidores. Acápite II, Examen de la Materia Auditada, numeral 9.b)	Fotografía N°2: Equipo de aire acondicionado y detalle de la instalación eléctrica. Acápite II, Examen de la Materia Auditada, numerales 9.f) y 9.h)
	
Fotografía N°3: Acceso Departamento de Informática. Acápite II, Examen de la Materia Auditada, numeral 9.g)	Fotografía N°4: Ubicación sala de servidores dentro del Departamento de Informática. (señalada con flecha) Acápite II, Examen de la Materia Auditada, numeral 9.g)

Fuente: Elaboración propia realizado en base a los antecedentes proporcionados por don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro a través de correo electrónico de fecha 23 de septiembre de 2021.

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

Anexo N° 9: Equipos computacionales con licencia de office distinta a la adquirida

N°	Serie	Marca y Modelo	Nombre Equipo	Tipo Equipo	Situación Reportada	Versión Office Instalada
[redacted]				PC	En uso	Microsoft Office Professional Plus 2010
				PC	En uso	Microsoft Office Professional Plus 2010
				PC	En uso	Microsoft Office Standard 2010
				PC	En uso	Microsoft Office Standard 2010
				NTB	En uso	Microsoft Office Standard 2010
				PC	En uso	Microsoft Office Standard 2010
				PC	En uso	Microsoft Office Standard 2010
				PC	En uso	Microsoft Office Standard 2010
				PC	En uso	Microsoft Office Standard 2010
				PC	En uso	Microsoft Office Standard 2010
				PC	En uso	Microsoft Office Standard 2010
				PC	Préstamo	Microsoft Office Standard 2010
				PC	En uso	Microsoft Office Standard 2010

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

Anexo N° 9: Equipos computacionales con licencia de office distinta a la adquirida (continuación)

N°	Serie	Marca y Modelo	Nombre Equipo	Tipo Equipo	Situación Reportada	Versión Office Instalada
[redacted]				PC	En uso	Microsoft Office Standard 2010
				NTB	En uso	Microsoft Office Standard 2010
				NTB	Préstamo	Microsoft Office Standard 2007

Fuente: Elaboración propia realizado en base a las validaciones efectuadas y a los antecedentes proporcionados por don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro a través de correo electrónico de fecha 23 de septiembre de 2021.

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

Anexo N° 10: Utilización de otros softwares no autorizados.

N°	Serie	Marca y Modelo	Nombre Equipo	Tipo Equipo	Situación Reportada	Software Instalado
[redacted]				PC	En uso	Adobe Acrobat XI Pro
				PC	En uso	Adobe Acrobat XI Pro
				PC	En uso	Adobe Acrobat XI Pro
				PC	En uso	uTorrent, Adobe Acrobat XI Pro, Adobe Photoshop CS6
				PC	En uso	Adobe Acrobat XI Pro
				PC	En uso	Adobe Acrobat XI Pro
				PC	En uso	Adobe Acrobat XI Pro
				PC	En uso	Adobe Acrobat XI Pro
				PC	En uso	Adobe Acrobat X Pro, Adobe Audition 1.5, Adobe creative suite master collection, utorrent, jdownloader 0.9, Microsoft Project Profesional 2010, Microsoft Visio Premium 2010
				PC	En uso	utorrent
				NTB	En uso	Adobe Acrobat XI Pro

Fuente: Elaboración propia realizado en base a las validaciones efectuadas y a los antecedentes proporcionados por don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro a través de correo electrónico de fecha 23 de septiembre de 2021.

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

Anexo N° 11: Equipos con Antivirus/Antimalware Básico.

N°	Serie	Marca y Modelo	Nombre Equipo	Tipo	Sistema Operativo	Antivirus/Antimalware
[redacted]				PC	WIN 7 PRO	Microsoft Security Essentials
				PC	WIN 7 PRO	Avast Free Antivirus
				PC	WIN 10 HOME SL	Windows Defender
				PC	WIN 10 HOME SL	Microsoft Defender
				NTB	WIN 7 PRO	Microsoft Security Essentials
				PC	WIN 10 PRO	Microsoft Defender
				PC	WIN 7 PRO	Microsoft Security Essentials
				PC	WIN 7 PRO	Microsoft Security Essentials
				PC	WIN 7 PRO	Microsoft Security Essentials
				PC	WIN 7 PRO	Microsoft Security Essentials
				PC	WIN 7 PRO	Microsoft Security Essentials
				PC	WIN 7 PRO	Microsoft Security Essentials

Anexo N° 11: Equipos con Antivirus/Antimalware Básico. (continuación)

N°	Serie	Marca y Modelo	Nombre Equipo	Tipo	Sistema Operativo	Antivirus/Antimalware
[redacted]				NTB	WIN 7 PRO	Microsoft Security Essentials
				PC	WIN 7 PRO	Microsoft Security Essentials
				PC	WIN SERVER 2008 R2 STANDARD	Malwarebytes gratis, elementos en cuarentena: 334
				NTB	WIN 7 PRO	AVG Free
				PC	WIN 7 PRO	Avira Free

Fuente: Elaboración propia realizado en base a las validaciones efectuadas y a los antecedentes proporcionados por don [redacted], Jefe del Departamento de Informática de la Municipalidad de Diego de Almagro a través de correo electrónico de fecha 23 de septiembre de 2021.

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

Anexo N° 12: Estado de observaciones de informe final N° 1.022, de 2021

Nº DE OBSERVACIÓN	MATERIA DE LA OBSERVACIÓN	COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN SOLICITADA POR CONTRALORÍA GENERAL EN INFORME FINAL	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DE LA ENTIDAD
Acápite I, Aspectos de Control Interno, numerales 1.1 y 1.2	Sobre manuales de procedimientos sin formalizar y Sobre manual de procedimiento desactualizado	Medianamente compleja (MC)	El servicio deberá remitir el manual de procedimientos de informática y el manual de procedimiento para el alta, baja y cambio de usuarios que trabajan con los Sistemas de Información Financiera Municipal, SIFIM, y Mercado Público debidamente actualizado y formalizado, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite I, Aspectos de Control Interno, numerales 1.3	Sobre falta de cumplimiento a las disposiciones contenidas en manuales de procedimiento	Medianamente compleja (MC)	El servicio deberá emitir un informe con las gestiones realizadas tendientes a subsanar las observaciones descritas en el Anexo N° 1, adjuntando respaldo de las difusiones al personal a través de correos electrónicos, registro de capacitaciones y actas de entrega de documentación, además de abordar las responsabilidades que le competen al Departamento de Informática sobre la materia observada, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe..			
Acápite II, Examen de la Materia Auditada, numeral 2.1	Sobre Ausencia de un inventario de activos de tecnologías de la información	Medianamente compleja (MC)	El servicio deberá remitir el inventario de los activos computacionales -hardware y software-, debidamente registrados con códigos de inventario asignados por la institución, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			

Anexo N° 12: Estado de observaciones de informe final N° 1.022, de 2021 (continuación)

Nº DE OBSERVACIÓN	MATERIA DE LA OBSERVACIÓN	COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN SOLICITADA POR CONTRALORÍA GENERAL EN INFORME FINAL	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DE LA ENTIDAD
Acápite II, Examen de la Materia Auditada, numeral 3.a)	Falta de designación del Encargado de Seguridad de la Información	Medianamente compleja (MC)	La entidad deberá remitir la designación formal del Encargado de Seguridad de la Información, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 3.b)	Inexistencia de un Comité de Seguridad de la Información	Medianamente compleja (MC)	La entidad deberá remitir la designación formal del Comité de Seguridad de la Información, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numerales 4.a) y 4.b)	Ausencia de política de seguridad de la información y Contenido de la política de seguridad de la información	Medianamente compleja (MC)	La entidad remitir la política de seguridad de la información, la cual tendrá que ser acreditada en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 4.c.a)	Referente al proceso de adquisición e instalación de equipos	Medianamente compleja (MC)	El municipio, deberá remitir un documento oficial que señale las responsabilidades sobre la adquisición, registro del inventario, instalación, habilitación, configuración e implementación de recursos informáticos, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			

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

ANEXO N° 12: Estado de observaciones de informe final N° 1.022, de 2021 (continuación)

Nº DE OBSERVACIÓN	MATERIA DE LA OBSERVACIÓN	COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN SOLICITADA POR CONTRALORÍA GENERAL EN INFORME FINAL	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DE LA ENTIDAD
Acápite II, Examen de la Materia Auditada, numeral 4.c.b)	Respecto del uso del correo institucional	Medianamente compleja (MC)	El servicio, deberá remitir los respaldos de las difusiones y/o capacitaciones realizadas con respecto de los riesgos asociados al uso del correo electrónico institucional, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 4.d)	Información no proporcionada	Medianamente compleja (MC)	El servicio, deberá remitir las últimas 5 solicitudes de alta/baja y/o modificación de usuarios SIFIM debidamente regularizadas o presentar un documento oficializado que actualice lo descrito en el manual de procedimiento para el alta, baja y cambio de usuarios que trabajan con los Sistemas de Información Financiera Municipal, SIFIM, y Mercado Público, autorizado mediante acta de acuerdo N° 79, del Concejo Municipal, de fecha 8 de mayo de 2012, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 5.a)	Ausencia de evaluación de riesgos	Medianamente compleja (MC)	La Municipalidad, deberá remitir el informe de evaluación de riesgos, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			

ANEXO N° 12: Estado de observaciones de informe final N° 1.022, de 2021 (continuación)

Nº DE OBSERVACIÓN	MATERIA DE LA OBSERVACIÓN	COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN SOLICITADA POR CONTRALORÍA GENERAL EN INFORME FINAL	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DE LA ENTIDAD
Acápite II, Examen de la Materia Auditada, numeral 6.a)	Clasificación y control de bienes	Medianamente compleja (MC)	La entidad comunal, deberá remitir el catastro de equipos computacionales del departamento de Informática actualizado y con las correcciones necesarias para subsanar la observación, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 6.b)	Ausencia de un catastro de software en inventario de activos de tecnologías de la información	Medianamente compleja (MC)	El servicio, deberá remitir el catastro de software que incluya las licencias adquiridas y las instaladas, indicando el usuario que le fue asignado, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 6.c)	Inconsistencias en el catastro de activos de tecnologías de la información	Medianamente compleja (MC)	La entidad, deberá remitir el catastro de equipos computacionales con todas las correcciones necesarias para subsanar la observación, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			

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

ANEXO N° 12: Estado de observaciones de informe final N° 1.022, de 2021 (continuación)

Nº DE OBSERVACIÓN	MATERIA DE LA OBSERVACIÓN	COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN SOLICITADA POR CONTRALORÍA GENERAL EN INFORME FINAL	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DE LA ENTIDAD
Acápite II, Examen de la Materia Auditada, numeral 7.a)	Sobre configuración de cuentas de usuarios en Windows con privilegios de administrador	Medianamente compleja (MC)	La Municipalidad de Diego de Almagro, deberá remitir la aclaración por los cuatro equipos computacionales asignados a los usuarios [redacted] los cuales no tienen instalado el sistema Cas Chile y sin embargo mantienen cuenta con privilegios administrativos, y además, remitir un documento del proveedor CAS Chile que certifique que las cuentas de usuario Windows deben ser configuradas con privilegios de administrador para el manejo de sus sistemas, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 7.b)	Sobre utilización de cuentas de usuarios genéricas en Windows	Medianamente compleja (MC)	El servicio, deberá dar cuenta de la regularización de los 17 casos observados, a través de una captura de pantalla de la cuenta de usuario donde se identifique el funcionario que tiene asignado el equipamiento, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 7.c)	Sobre irregularidades en las cuentas de usuarios en sistema SIFIM	Medianamente compleja (MC)	El municipio, deberá remitir una nueva nómina en formato Excel (xls o xlsx) con las cuentas de usuario del Sistema SIFIM, en donde se evidencie las modificaciones y/o eliminaciones, además de un certificado firmado que respalde el archivo digital, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			

ANEXO N° 12: Estado de observaciones de informe final N° 1.022, de 2021 (continuación)

Nº DE OBSERVACIÓN	MATERIA DE LA OBSERVACIÓN	COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN SOLICITADA POR CONTRALORÍA GENERAL EN INFORME FINAL	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DE LA ENTIDAD
Acápite II, Examen de la Materia Auditada, numeral 7.d)	Respecto de la configuración de contraseñas	Medianamente compleja (MC)	La entidad, deberá remitir las gestiones realizadas con el proveedor de sistemas para modificar la extensión y complejidad de las contraseñas para dar cumplimiento de la normativa, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 7.e)	Sobre período de actualización de contraseñas	Medianamente compleja (MC)	La entidad comunal, deberá definir el procedimiento para cambiar los identificadores a intervalos regulares y comunicar las adecuaciones en la plataforma tecnológica, indicando el usuario que le fue asignado, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 7.f)	Equipos computacionales con acceso liberado	Medianamente compleja (MC)	El servicio, deberá remitir las capturas de pantalla que den cuenta de la identificación del usuario y el bloqueo de redes sociales, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numerales 9.a) y 9.i)	Ausencia de bitácoras de acceso a sala de servidores	Medianamente compleja (MC)	La entidad municipal, deberá remitir evidencia de la puesta en marcha de una bitácora física, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			

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

ANEXO N° 12: Estado de observaciones de informe final N° 1.022, de 2021 (continuación)

Nº DE OBSERVACIÓN	MATERIA DE LA OBSERVACIÓN	COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN SOLICITADA POR CONTRALORÍA GENERAL EN INFORME FINAL	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DE LA ENTIDAD
Acápite II, Examen de la Materia Auditada, numerales 9.b), 9.c), 9.d), 9.g) y 9.h)	Inexistencia de puerta de cortafuego, Inexistencia de sistemas de emergencia en sala de servidores, Falta de sistema de iluminación de emergencia, Sobre seguridad implementada en sala de servidores, Sobre instalaciones eléctricas en sala de servidores	Medianamente compleja (MC)	La Municipalidad de Diego de Almagro, deberá remitir un plan de mejora para la sala de servidores que incluya la instalación, mejora o modificación de los elementos observados, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 9.e)	Sobre señalética en sala de servidores	Medianamente compleja (MC)	La entidad edilicia, deberá remitir las fotografías que den cuenta de la habilitación de carteles en lugares visibles que establezcan las prohibiciones de fumar, consumir alimentos y/o bebidas, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 9.f)	Referente a equipo de ventilación en sala de servidores	Medianamente compleja (MC)	El servicio, deberá remitir el estado de habilitación y funcionamiento del equipo de aire acondicionado para subsanar la observación, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			

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

ANEXO N° 12: Estado de observaciones de informe final N° 1.022, de 2021 (continuación)

Nº DE OBSERVACIÓN	MATERIA DE LA OBSERVACIÓN	COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN SOLICITADA POR CONTRALORÍA GENERAL EN INFORME FINAL	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DE LA ENTIDAD
Acápite II, Examen de la Materia Auditada, numeral 10.a)	Procedimientos de destrucción de información	Medianamente compleja (MC)	La entidad, deberá remitir los procedimientos formales relacionados con los procesos de destrucción de información de los equipos en desuso, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 10.b)	Controles criptográficos	Medianamente compleja (MC)	El servicio, deberá definir y comunicar formalmente cuál es la información sensible afecta a ser cifrada en la base de datos del sistema SIFIM, o en su defecto, comunicar el respaldo de las gestiones con el proveedor de software para cifrar los datos contenidos en las tablas de datos, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 11.a)	Utilización de licencias de Microsoft Office no autorizadas	Medianamente compleja (MC)	La entidad, deberá remitir el contrato con la empresa Microsoft que acredite la disponibilidad de las descargas para realizar el downgrade a los equipos informáticos del Municipio, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			

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

ANEXO N° 12: Estado de observaciones de informe final N° 1.022, de 2021 (continuación)

Nº DE OBSERVACIÓN	MATERIA DE LA OBSERVACIÓN	COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN SOLICITADA POR CONTRALORÍA GENERAL EN INFORME FINAL	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DE LA ENTIDAD
Acápite II, Examen de la Materia Auditada, numeral 11.b)	Compra de licencias de software Microsoft Office no instaladas	Medianamente compleja (MC)	La Municipalidad de Diego de Almagro, deberá remitir un plan de renovación de equipos computacionales que permitan la instalación del software adquirido, que incluya responsables y plazos concretos para su ejecución, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 11.c)	Utilización de otros softwares no autorizados	Medianamente compleja (MC)	La entidad, deberá remitir las capturas de pantalla del panel de control que evidencie la eliminación del software, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 12.a)	Ambientes de producción y prueba	Medianamente compleja (MC)	La entidad, deberá remitir las evidencias que respalden la habilitación de un ambiente de prueba en el servidor SIFIM, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numerales 12.b.a) y 12.b.b)	Referente a la infraestructura tecnológica implementada por la entidad y Sobre sistemas de protección del servidor SIFIM	Medianamente compleja (MC)	El ente edilicio, deberá remitir un informe sobre la habilitación del equipo firewall que indica, además de un plan de mejora a su infraestructura tecnológica que incluya la adquisición de un software antivirus, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			

ANEXO N° 12: Estado de observaciones de informe final N° 1.022, de 2021 (continuación)

Nº DE OBSERVACIÓN	MATERIA DE LA OBSERVACIÓN	COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN SOLICITADA POR CONTRALORÍA GENERAL EN INFORME FINAL	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DE LA ENTIDAD
Acápite II, Examen de la Materia Auditada, numeral 12.c)	Ausencia de un plan de continuidad	Medianamente compleja (MC)	El servicio, deberá remitir un plan de continuidad que establezca los procedimientos para la recuperación ante los potenciales ataques de código malicioso, que incluya todos los datos y software necesarios de respaldo, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 12.d)	Equipos con Microsoft Windows sin actualizar	Medianamente compleja (MC)	La entidad comunal, deberá remitir un informe con el estado de actualización de estos equipos, el cual incluya fundamentos técnicos de que los equipos no cumplen con las condiciones de hardware para recibir actualizaciones y un plan de renovación de equipos computacionales que incluya responsables y plazos concretos para su ejecución, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 13.a)	Información no proporcionada	Medianamente compleja (MC)	El servicio, deberá remitir el convenio actual de SIFIM y una aclaración de las responsabilidades que deben ser atribuidas al municipio o a la empresa GTD sobre los procesos de copias de seguridad y restauración de sus sistemas, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			

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

ANEXO N° 12: Estado de observaciones de informe final N° 1.022, de 2021 (continuación)

Nº DE OBSERVACIÓN	MATERIA DE LA OBSERVACIÓN	COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN SOLICITADA POR CONTRALORÍA GENERAL EN INFORME FINAL	MEDIDA IMPLEMENTADA Y SU DOCUMENTACIÓN DE RESPALDO	FOLIO O NUMERACIÓN DOCUMENTO DE RESPALDO	OBSERVACIONES Y/O COMENTARIOS DE LA ENTIDAD
Acápite II, Examen de la Materia Auditada, numerales 13.b) y 13.c)	Copias de seguridad, Referente al proceso de restauración de base de datos	Medianamente compleja (MC)	La entidad edilicia, deberá remitir la política de respaldo formal de sus sistemas la cual contenga al menos, los procedimientos técnicos de copias de seguridad y restauración, estrategias ante contingencias, planificación de ensayos de restauración y responsables. Además de adjuntar, para el caso del numeral 13.c), las capturas de pantalla de la restauración a la última copia de seguridad generada, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 13.d)	Registro de fallas (logs)	Medianamente compleja (MC)	El servicio, deberá remitir el procedimiento de registro de fallas debidamente formalizado, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			
Acápite II, Examen de la Materia Auditada, numeral 13.e)	Vulnerabilidades de los sistemas informáticos	Medianamente compleja (MC)	El servicio, deberá dar cuenta de la atención de estas vulnerabilidades, lo cual tendrá que ser acreditado en el Sistema de Seguimiento y Apoyo CGR, en el plazo de 60 días hábiles, contado desde la fecha de recepción del presente informe.			