POR EL CUIDADO Y BUEN USO
DE LOS RECURSOS PÚBLICOS

CONTRALORÍA REGIONAL DE LA ARAUCANÍA
UNIDAD DE CONTROL EXTERNO

INFORME FINAL

MUNICIPALIDAD DE ANGOL

INFORME N° 927/2022
28 DE DICIEMBRE DE 2022

OBJETIVOS DE DESARROLLO SOSTENIBLE

OBJETIVOS DE DESARROLLO SOSTENIBLE

CONTRALORÍA GENERAL DE LA REPÚBLICA CHILE

POR EL CUIDADO Y BUEN USO DE LOS RECURSOS PÚBLICOS

ÍNDICE

RESUMEN EJECUTIVO

Informe Final de Auditoría N° 927, de 2022

Municipalidad de Angol.

Objetivo: efectuar una auditoría a en la Municipalidad de Angol, con la finalidad de revisar y evaluar el nivel de seguridad informática implementado por la entidad, en el periodo comprendido entre 1 de marzo de 2021 al 30 de noviembre de 2022.

Preguntas de Auditoría:

- ¿La entidad ha implementado controles para la gestión de la seguridad de la información?
- ¿Los sistemas de tecnologías de información actuales permiten al municipio dar continuidad a sus funciones considerando el teletrabajo?

Principales resultados:

Se constataron una serie de deficiencias en los sistemas de información mantenidos por la Municipalidad de Angol, lo que no se aviene con lo establecido en el decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los Órganos del Estado sobre la seguridad y confidencialidad de los documentos electrónicos, entre las que se destacan las siguientes:

- Se corroboró que la municipalidad no ha efectuado una evaluación de los riesgos asociados a la seguridad de la información, respecto de los sistemas informáticos que posee. Asimismo, se estableció que no cuentan con una política de seguridad de la información. Del mismo modo, se detectaron deficiencias en los respaldos de seguridad de la información. Además, se comprobó que el municipio no cuenta con un funcionario encargado de seguridad de la información.
- Se evidenciaron deficiencias en las bases de inventario y la administración de los bienes de activos de TI. En efecto, se constató que el municipio no ha elaborado un catastro con el inventario de los activos de información situación que no permitió acreditar qué funcionario es el responsable de su custodia.
- Se verificaron ausencias de controles de acceso lógico y la inexistencia de políticas y procedimientos de acceso remoto para el uso de redes y servicios en red, en el desarrollo de labores de teletrabajo. Además, de la ausencia de controles sobre la instalación de software no autorizado en los equipos informáticos de dicha entidad.

  Con el objeto de subsanar, entre otras observaciones, lo indicado precedentemente, el municipio remitió el documento denominado “Carta Gantt auditoría de seguridad de la información”, el cual contempla una serie de actividades a desarrollar durante el año 2023, cuyas acciones deberá acreditar documentadamente ante este Organismo de Control en el plazo de 60 días hábiles, contado desde la recepción del presente informe.

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

PREG N° 9.075/2022
AT N° 217/2022

INFORME FINAL DE AUDITORÍA N° 927, DE 2022, SOBRE FISCALIZACIÓN A LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN EN LA MUNICIPALIDAD DE ANGOL.

TEMUCO, 28 de diciembre de 2022

Esta Contraloría Regional, en cumplimiento de su plan anual de fiscalización para el año 2022, y en conformidad con lo dispuesto en la ley N° 10.336, de Organización y Atribuciones de esta institución, se efectuó una auditoría a los sistemas de información mantenidos en la Municipalidad de Angol, con la finalidad de revisar y evaluar el nivel de seguridad informática implementado por la entidad, en el periodo comprendido entre 1 de marzo de 2021 al 30 de noviembre de 2022.

JUSTIFICACIÓN

A partir de la ejecución de auditorías de sistemas desarrolladas por esta Contraloría General de la República, se han advertido deficiencias en los sistemas informáticos mantenidos por los servicios públicos que afectan la seguridad y confiabilidad de estos y de la información que generan y resguardan. Asimismo, en 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 que conforman a la Administración del Estado.

Además de lo anterior, a través de la presente revisión, 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.

ANTECEDENTES GENERALES

La Municipalidad de Angol es una corporación de derecho público, con personalidad jurídica y patrimonio propio, cuya finalidad es satisfacer las necesidades de la comunidad local y asegurar su

AL SEÑOR
MARCELLO LIMONE MUÑOZ
CONTRALOR REGIONAL DE LA ARAUCANÍA
PRESENTE

participación en el progreso económico, social y cultural de la comuna, según dispone el artículo 1° de la ley N° 18.695, Orgánica Constitucional de Municipalidades. Dicha entidad está constituida por el alcalde, que es su máxima autoridad, quien ejerce la dirección y administración superior y la supervigilancia de su funcionamiento y por el concejo municipal, órgano colegiado de carácter normativo, resolutivo y fiscalizador, encargado de hacer efectiva la participación de la comunidad local y de ejercer las atribuciones que señala la precitada ley.

Sobre la materia, 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, que Aprueba Norma Técnica para los Órganos del Estado sobre la Seguridad y Confidencialidad de los Documentos Electrónicos, 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 - códigos 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.

Respecto de la aplicación de la Norma Chilena ISO 27.002, de 2009, cabe agregar que conforme al dictamen N° 2.643, de 2013, de esta Contraloría General se ha reconocido el carácter vinculante de las normas oficiales chilenas cuando éstas han sido declaradas mediante decreto supremo publicado en el Diario Oficial, como ocurre en la especie.

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.

Cabe mencionar que a través del oficio electrónico N° E285922, de 9 de diciembre de 2022, de esta Sede Regional, con carácter de confidencial fue puesto en conocimiento de la autoridad, el preinforme de auditoría N° 927, de igual año, con la finalidad que formulara los alcances y precisiones que, a su juicio, procedieran, lo que se concretó mediante el oficio ordinario N° 2.764/575, de 19 de diciembre, de la misma anualidad.

Sin perjuicio de lo anterior, cabe indicar que, en dicho escrito de respuesta, la autoridad comunal remite el documento denominado “Carta Gantt auditoría de seguridad de la información”, en adelante el plan, el cual contempla una serie de actividades a desarrollar durante el periodo 2023, a fin de poder subsanar cada una de las observaciones contenidas en el presente informe final, cuyo detalle se presenta en el anexo N° 1 del presente informe.

OBJETIVO

Efectuar una auditoría al macroproceso de Tecnologías de la Información, TI, con la finalidad de revisar y evaluar el nivel de seguridad informática implementado por la Municipalidad de Angol, 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 anotado decreto N° 83, de 2004, en el periodo comprendido entre 1 de marzo de 2021 al 30 de noviembre de 2022.

METODOLOGÍA

La revisión se efectuó de acuerdo con la Metodología de Auditoría de esta Entidad Fiscalizadora contenida en la resolución N° 10, de 2021, que fija normas que regulan las auditorías efectuadas por la Contraloría General de la República, y con los procedimientos de control sancionados por la resolución exenta N° 1.485, de 1996, que aprueba normas de control interno, de este Organismo de Fiscalización, considerando la evaluación de control interno, la ejecución de pruebas de validación, análisis de la información recopilada, y entrevistas con el personal responsable, entre otras 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 al levantamiento de información efectuado, el universo de sistemas que mantiene el servicio se muestra a continuación:

Tabla N° 1: Universo y muestra.

Denominación del sistema	Tipo de desarrollo de sistema
Sistema de Gestión Municipal CASCHILE	Arrendado
Cementerio Municipal	Propio
Veterinaria Municipal	Propio
Denuncia Ciudadana (Seguridad Publica)	Propio

Fuente elaboración propia a partir de la información proporcionada por don [redacted] Encargado de Unidad de Informática en reunión de inicio, 08 de julio de 2022.

En virtud del objetivo de la auditoría, esta Entidad de Control contempló validaciones sobre el referido sistema informático.

RESULTADOS DE LA AUDITORÍA

Del examen efectuado, se determinaron las siguientes situaciones:

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. Situaciones de riesgo no controlados por el servicio.

1.1. Ausencia de evaluación de riesgos de seguridad de la información.

Se observó que el municipio no ha efectuado una evaluación de los riesgos asociados a la seguridad de la información, respecto de los sistemas de informáticos que posee, dicha situación vulnera lo establecido en el artículo 8°, del citado decreto N° 83, de 2004, el cual señala que los órganos de la Administración regidos por esta norma deberán aplicar sus disposiciones para garantizar los atributos esenciales que confieren seguridad al documento electrónico, definidos en el artículo 6°. No obstante, la consecución y mantención de tales atributos por parte de cada órgano de la Administración del Estado estarán sujetas a la consideración de factores de riesgo y factores de costo/beneficio. Estos últimos podrán invocarse mediante una resolución fundada del jefe de servicio correspondiente, basada en un estudio de análisis de riesgo y/o costo/beneficio.

Por último, lo descrito no se encuentra en armonía con lo previsto en la citada resolución exenta N° 1.485, de 1996, normas generales, letra e), vigilancia de los controles, numeral 38, en cuanto a que los directivos deben vigilar continuamente sus operaciones y adoptar inmediatamente las medidas oportunas ante cualquier evidencia de irregularidad o de actuación contraría a los principios de economía, eficiencia y eficacia.

En su respuesta, el municipio reconoce la situación detectada, agregando -en síntesis- que se compromete a realizar una evaluación de los riesgos de seguridad de la información, la cual se realizará a través de un mecanismo de matriz, el cual estará dirigido a estimar la magnitud de los riesgos que no hayan podido evitarse, proporcionando al municipio la información necesaria para decidir sobre la necesidad de adoptar medidas adecuadas para garantizar la seguridad y protección de la información.

Así entonces, y atendido a que en su respuesta el municipio alude a medidas que aún no se concretan, pues ellas se aplicarán en el futuro, se mantiene la situación objetada, por lo que ese municipio deberá remitir el reporte con los resultados de la aplicación de la evaluación de los riesgos de seguridad de la información, en un plazo de 60 días hábiles por medio del Sistema de Seguimiento y Apoyo CGR, a contar de la recepción del presente informe, instancia en la que se evaluará la efectividad de lo obrado.

1.2. Ausencia de cláusulas de verificación sobre controles de acceso, respaldo de datos, continuidad de negocio y niveles de servicios, en prestaciones contratados.

Sobre la materia, se constató que los principales servicios informáticos de la Municipalidad de Angol se encuentran externalizados, según lo informado por el encargado de informática de la entidad edilicia señor [redacted] Al respecto, el aludido funcionario remitió las facturas de prestación de los servicios Hosting de Tecnologiachile.com Limitada y los contratos de servicio de telecomunicaciones y de correo de Google Workspace sublicenciado por Entel y con CASCHILE S.A por el uso de su programa de gestión municipal, vigentes por el periodo en curso.

Del examen a las condiciones, de los referidos convenios, se advirtió en el servicio de Tecnologiachile.com Ltda. y con CASCHILE S.A., de este último, el contrato denominado "Licencia de uso temporal de programas computaciones", la ausencia de cláusulas de seguridad respecto de los controles de acceso, respaldo de datos, continuidad de negocio y niveles de servicios asociados a multas.

Al respecto, cabe indicar que la ausencia de cláusulas de seguridad respecto de los controles de acceso, respaldo de datos, continuidad de negocio, se debe tener en consideración el inciso primero del artículo 20 del reglamento de la ley N° 19.886, de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios, aprobado por el decreto N° 250, de 2004, que dispone que las bases de licitación deberán establecer las condiciones que permitan alcanzar la combinación más ventajosa entre todos los beneficios del bien o servicio por adquirir y todos sus costos asociados, presentes y futuros.

Luego, el inciso segundo agrega que la Entidad Licitante no atenderá sólo al posible precio del bien y/o servicio, sino a todas las condiciones que impacten en los beneficios o costos que se espera recibir del bien y/o servicio. En la determinación de las condiciones de las Bases, la Entidad Licitante deberá propender a la eficacia, eficiencia, calidad de los bienes y servicios que pretende contratar y ahorro en sus contrataciones.

A su turno, el artículo 22, N° 2, del referido decreto contempla como contenido mínimo de las bases, entre otros, las especificaciones de los bienes y/o servicios que se quieren contratar, las cuales deberán ser genéricas, sin hacer referencia a marcas específicas. Como puede advertirse, de conformidad con la normativa citada, al elaborar las bases las entidades licitantes pueden exigir el cumplimiento de los requisitos técnicos que consideren pertinentes de acuerdo con la naturaleza de los bienes o servicios que pretenden contratar, de manera que la determinación de los estándares que deben concurrir en cada caso es un asunto que compete decidir a la repartición pública que licita, ponderando las necesidades que en cada caso pretende satisfacer por esa vía (aplica criterio contenido en el dictámenes N^{os}14.250, de 2018 y E240654, de 2022, ambos de esta Entidad Fiscalizadora)

Por su parte, en lo referido a la carencia de estipulaciones de seguridad en los niveles de servicio, asociadas a multas, cabe recordar que el inciso tercero del artículo 11 de la ley N° 19.886, establece que con cargo a la garantía que asegure el fiel y oportuno cumplimiento del contrato podrán hacerse efectivas las multas y demás sanciones que afecten a los contratistas, disposición que es reiterada en el N° 6 del artículo 22 del reglamento de dicho texto legal, aprobado por el decreto N° 250, de 2004, el cual reconoce la posibilidad de que la Administración contemple multas en las contrataciones que celebre a título oneroso para el suministro de bienes y servicios, en la eventualidad que el proveedor incurra en el incumplimiento de las obligaciones contraídas.

En ese contexto, el dictamen N° 78.037, de 2013, de esta Institución Contralora, expresa que la normativa reconoce la posibilidad de que la Administración contemple multas en las contrataciones que celebre a título oneroso para el suministro de bienes y servicios, en la eventualidad que el proveedor incurra en el incumplimiento de las obligaciones contraídas. De esta manera, corresponde a la propia entidad pública fijar en el respectivo pliego de condiciones las infracciones contractuales del adjudicatario que darán lugar a la aplicación de multas y el monto de estas últimas, tratándose de licitaciones públicas y privadas, o velar por la incorporación al contrato de disposiciones que regulen la materia, en los casos de adquisiciones por trato directo, con el objeto de resguardar los intereses públicos comprometidos en dichas convenciones, lo que no se habría efectuado en la especie.

Las situaciones descritas infringen lo dispuesto en la letra b), del artículo 37, sobre seguridad organizacional, referente a lo señalado en el acápite 6.2.3, de la norma chilena NCh-ISO 27.002, de 2009, sobre tener en cuenta la seguridad en los acuerdos con terceras partes.

Además, vulnera los principios de eficiencia y eficacia consagrados en los artículos 3°, 5° y 8° de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado y 6° de la citada ley N° 19.886, que exigen a las autoridades y funcionarios, en sus contrataciones, velar por la eficiente e idónea administración de los medios públicos (aplica criterio contenido en los dictámenes N^{os} 3.160 y 87.444, ambos de 2015, y 29.217, de 2016, todos de esta Entidad de Control).

Por último, no se aviene con lo previsto en la resolución exenta N° 1.485, de 1996, normas generales, letra e), vigilancia de los

controles, numeral 38, en cuanto a que los directivos deben vigilar continuamente sus operaciones y adoptar inmediatamente las medidas oportunas ante cualquier evidencia de irregularidad o de actuación contraría a los principios de economía, eficiencia y eficacia.

Sobre lo objetado, en su respuesta, el municipio señala que, respecto a estas situaciones observadas, ellas serán requeridas en los futuros procesos de licitación o mediante peticiones formales a los proveedores establecidos, labor que está planificada en el plan, el cual confeccionó en base a la hoja de ruta ISO 27001, sobre Seguridad de la Información.

Atendido a que en su contestación, el municipio reconoce lo observado y alude a medidas que aún no se concretan, pues ellas se aplicarán en el futuro, se mantienen las situaciones objetadas, por lo tanto, esa entidad municipal deberá hacer efectiva las medidas informadas, esto es, requerir en los futuros procesos de licitación o mediante peticiones formales a los proveedores establecidos, según se encuentra planificado en el plan adjunto, a fin de evitar de que dichas situaciones se repitan en el futuro, lo cual deberá acreditar documentadamente ante la Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

Asimismo, es necesario que el referido procedimiento se mantenga en el tiempo a fin de dar cumplimiento a lo establecido a lo establecido en los artículos 11 y 22 de la citada ley N° 19.886 y su reglamento aprobado por el decreto N° 250, de 2004, respectivamente.

II. EXAMEN DE LA MATERIA AUDITADA

2. Listado de funcionarios desvinculados y cambiados de funciones no puestos a disposición para el examen.

Sobre el particular, cabe indicar que al cierre de la presente auditoría el municipio no puso a disposición los antecedentes referidos a la nómina de funcionarios desvinculados y cambiados de función en los últimos 3 meses, a saber, septiembre, octubre y noviembre, todos del año 2022, situación que no permitió efectuar una validación a los controles establecidos -por la entidad auditada- en la letra c) sobre acceso a la red de datos, del Reglamento de Uso y Seguridad de la Plataforma Tecnológica, de la Municipalidad de Angol, el cual fue aprobado mediante el decreto alcaldicio N° 2.189/114, de 21 de noviembre de 2021.

Lo descrito precedentemente, transgrede lo consignado en los artículos 9°, 85 y 91, de la referida ley N° 10.336, que, en síntesis, en lo que interesa, señalan que este Organismo de Control podrá solicitar de cualquier funcionario los datos e informaciones que necesite para el mejor desempeño de sus labores, quienes están obligados a proporcionarlos, quedando sujetos a las medidas de apremio que allí se indican.

Por último, vulnera lo prescrito en el artículo 17 de la mencionada resolución N° 10, de 2021, de esta Entidad de Control, 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 citada 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.

El municipio manifiesta que se establecerá como procedimiento de manera trimestral, preparar y tener disponible dicha información. Asimismo, remite copia del memorándum N° 131, de 1 de diciembre de 2022, de la directora de Recursos Humanos del municipio, por medio del cual informa la nómina de funcionarios desvinculados por el periodo septiembre, octubre y noviembre de la citada anualidad.

Sin perjuicio de los argumentos expuestos, se mantiene la observación, por cuanto el municipio no remitió antecedentes sobre si los perfiles de acceso de los exfuncionarios se encuentran eliminados o vigentes, a la fecha, para acceder a la plataforma tecnológica de red de datos de dicha entidad edilicia.

Así entonces, esa entidad deberá comunicar sobre la efectividad o no de las medidas informadas, referidas al procedimiento de verificación de eliminación de perfiles de los funcionarios desvinculados y/o cambiados de funciones, a fin de generar las mejoraras informadas, lo que deberá ser acreditado en el plazo de 60 días hábiles, contado desde la entrega del presente informe.

3. Reglamento no establece la periodicidad de revisión.

Del análisis a los antecedentes entregados por el municipio, se advirtió el citado decreto alcaldicio N° 2.189/114, de 2021, que aprobó el reglamento de uso y seguridad de la plataforma tecnológica. Al respecto, cabe señalar que dicho instructivo tiene como propósito definir las políticas sobre el uso apropiado de las plataformas tecnológicas disponibles en el municipio, sin embargo, el aludido documento no establece la periodicidad de revisión y actualización o si se producen cambios significativos, de la información de dichas plataformas, para asegurar su conveniencia, suficiencia, y eficacias continuas.

Lo antes indicado, no se condice con lo señalado en el artículo 11 del mencionado decreto N° 83, de 2004, el que señala en su inciso segundo que, las políticas de seguridad deberán documentarse y explicitar la periodicidad con que su cumplimiento será revisado.

Esa entidad comunica que el referido reglamento se revisará con el objeto de dar cumplimiento a lo establecido en el artículo 11 del decreto N° 83, de 2004, por lo que se establecerá una política de renovación en un plazo de 1 año.

En virtud de lo contestado, y aludido que las medidas aún no se concretan, pues ellas se aplicarán en el futuro, se mantiene la situación objetada, por lo que ese municipio deberá establecer en el reglamento de uso y seguridad de la plataforma tecnológica la periodicidad de revisión y actualización o si se producen cambios significativos, de la información de dichas plataformas, para

asegurar su conveniencia, suficiencia, y eficacias continuas, lo que tendrá que informar el cumplimiento de lo indicado, en un plazo de 60 días hábiles en el Sistema de Seguimiento y Apoyo CGR, a contar de la recepción del presente informe.

4. Inexistencia de un encargado de seguridad de la información.

Se advirtió que el municipio no cuenta con un encargado u oficial de seguridad de la información, según lo exige el inciso primero del artículo 12, del referido decreto N° 83, de 2004, el cual establece, que en cada organismo regido por esta norma se deberá contar con un encargado de seguridad, quién actuará como asesor del jefe de la entidad respecto de las materias relativas a seguridad de los documentos electrónicos.

Asimismo, no se aviene con lo indicado en el numeral 6.1, de la mencionada norma NCh-ISO 27.002, de 2009, que señala, en lo que interesa, que se debe establecer un marco de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

5. Inexistencia de un comité de seguridad de la información.

Se advirtió que el municipio no tiene conformado un comité de seguridad de la información, con el objetivo de cooperar en estas materias al encargado u oficial de seguridad, según lo exige el artículo 4°, del referido decreto N° 83, de 2004, el cual establece, en lo que interesa, que los jefes de servicio deberán designar, un encargado de seguridad, para que desarrolle e implemente las políticas de seguridad en forma conjunta con el comité de gestión de seguridad y confidencialidad y en aquellos órganos en que no se designe, actuará como encargado de seguridad el auditor interno de cada servicio.

Sobre lo objetado, en los numerales 4 y 5, precedentes, el municipio señala, por una parte, que el nombramiento del encargado de seguridad se deberá efectuar dentro del proceso de mejora permanente, estableciendo un marco de gestión para iniciar y controlar la implementación de la seguridad de la información dentro del municipio y, por otra, que realizará la conformación de un comité de seguridad de la información la cual estará compuesto por funcionarios de distintas áreas. Ambos procesos se realizarán de conformidad a los plazos estipulados en el plan.

En atención a que la autoridad alude a medidas que aún no se concretan, pues ellas se materializarán en el futuro, se mantienen las situaciones objetadas.

Ahora bien, esa entidad edilicia deberá acreditar las acciones informadas referidas al nombramiento del funcionario para dicha labor, procurando que exista un control de oposición de funciones o de segregación de funciones en las labores del referido cargo, remitiendo la documentación pertinente ante esta Contraloría Regional. Del mismo modo, tendrá que emprender las medidas informadas, debiendo acreditar las acciones referidas a la creación de un comité de seguridad de información, remitiendo la documentación pertinente ante esta Contraloría Regional, ambas acciones deberá informarlas en el término de 60 días hábiles, contado desde la recepción del presente informe.

6. Ausencia de un inventario con el detalle de los activos de tecnologías de información, TI.

De las diligencias practicadas, en la visita a la municipalidad, se constató que esa entidad no tiene elaborado un catastro actualizado y completo del inventario de los activos de información. Lo expuesto, no se ajusta a lo establecido en la letra c), del artículo 37, del citado decreto N° 83, de 2004, sobre clasificación y control de bienes.

Además, contraviene el numeral 7.1 de la norma NCh-ISO 27.002, de 2009, la cual señala que se debe implementar y mantener una adecuada protección sobre los activos de la organización, y que todos los activos deberían tener un responsable y se debería asignar un dueño a cada uno de ellos.

En su escrito de respuesta, la autoridad comunal manifiesta que se cuenta con un inventario, el cual es administrado por la unidad de bienes e inventario. Asimismo, remitió un archivo con un detalle de los bienes TI.

Sin perjuicio de los argumentos expuestos, se mantiene la observación, puesto que conforme a lo establecido en la citada norma NCh-ISO 27.002, de 2009, el archivo proporcionado por el municipio, solo se remite a los activos físicos TI, y no contempla los activos de software dentro de dicha base de datos remitida, en su respuesta, lo cual se refuerza con los argumentos expuestos en la observación del numeral 18, diferencias entre activos TI y el licenciamiento de uso de software del presente informe.

En atención a lo expuesto, el municipio deberá actualizar la información del inventario informático municipal, remitiendo un informe con el reporte de los avances de los resultados obtenidos, en un plazo de 60 días hábiles a contar de la recepción del presente informe, instancia en la que se evaluará la efectividad de lo realizado.

7. Inexistencia de seguridad física para los servidores.

Sobre el particular, el día 22 de noviembre de 2022, se realizó una visita a las dependencias de la entidad auditada, con el propósito de verificar la seguridad a la sala de servidores y comunicaciones. Al respecto, las diligencias permitieron advertir que los servidores de datos se encuentran en un espacio contiguo a la oficina del encargado de informática, sin que exista algún perímetro sólido o sistema de seguridad que impida el paso a estos equipos.

Lo antes mencionado, incumple el artículo 19, letra a) del citado decreto N° 83, de 2004, el cual señala, en lo que interesa, que respecto de los documentos electrónicos de la organización clasificados como reservados o secretos, deberán almacenarse en áreas seguras, protegidos por un perímetro de seguridad definido, con barreras apropiadas de resguardo y controles de entrada, además, de estar físicamente protegidos del acceso no autorizado, daño e interferencia, asimismo, deberá guardar relación con los riesgos identificados, lo cual se condice con lo indicado en el numeral 9.1.1, relativo al perímetro de seguridad

física, y punto 9.2.1, sobre ubicación y protección del equipamiento de la norma técnica NCh-ISO 27.002, de 2009.

8. Ausencia de controles ambientales para la zona de servidores.

De las diligencias practicadas, en las instalaciones de los servidores de la entidad, se constató que estos no poseen equipos de aire acondicionado, monitores de temperatura, de humedad y sensores ambientales específicos para la ubicación de esos equipos computacionales, advirtiéndose solo un aparato de aire en el sector de la oficina anexa del encargado de informática.

Dichas situaciones, vulneran lo dispuesto en la letra b), del artículo 18 del aludido decreto N° 83, de 2004, que señala, en lo que corresponde, que cada órgano deberá impartir y publicitar instrucciones relativas a los aspectos del ambiente externo, respecto a las condiciones climatológicas y ambientales que pueden afectar sistemas informáticos o entornos cercanos.

Del mismo modo, no se condice con lo establecido en la letra f) del numeral 9.2.1. de la NCh ISO 27.002, de 2009, que señala 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 información.

Sobre los numerales 8 y 9, precedentes, el municipio indica que conforme a lo establecido en el plan se realizará la segmentación del área de servidores, dentro del plazo allí consignado, asimismo, la adquisición e implementación de equipos de aire para mejorar su calidad en la zona de servidores.

En virtud que las acciones informadas por el municipio, aún no se concretan, se mantienen las observaciones, por lo tanto esa entidad deberá emprender las medidas informadas, debiendo acreditar, por una parte, sobre la segmentación de las dependencias de los servidores y las áreas que correspondan, además de la instalación de los equipos de climatización, a fin de generar las mejoraras informadas, lo que deberá ser acreditado en el plazo de 60 días hábiles, contado desde la entrega del presente informe.

9. Deficiencia en suministro eléctrico para los servidores.

En la referida visita a terreno -22 de noviembre de 2022-, se inspeccionaron las instalaciones del suministro eléctrico para los servidores, respecto de lo cual se constató que éstas no están destinadas específicamente para estos equipos TI, puesto que estos se encuentran conectados a la red eléctrica normal del edificio, y no a un circuito para computación. Asimismo, el encargado de unidad de informática señaló que desconoce sobre el estado de funcionamiento y ciclo de vida de los equipos auxiliares, a saber, generadores eléctricos y UPS[1] o sistema de alimentación ininterrumpida.

[1] La sigla UPS es la abreviación de su nombre en inglés Uninterruptable Power Supply, también llamado Sistema de Alimentación Ininterrumpida (SAI). Dicho dispositivo permite tener flujo de energía eléctrica mediante baterías, cuando el suministro eléctrico falla.

Las situaciones expuestas, infringen lo establecido en el artículo 17, del aludido decreto N° 83, de 2004, el cual señala que los equipos deberán protegerse físicamente de las amenazas de riesgos del ambiente externo, pérdida o daño, incluyendo las instalaciones de apoyo tales como el suministro eléctrico y la infraestructura de cables. En particular, la ubicación del equipamiento de la institución deberá minimizar el acceso innecesario a las áreas de trabajo y disminuir las posibilidades de amenazas de humo y fuego, humedad y agua, inestabilidad en el suministro eléctrico, hurto y robo, lo cual se condice con lo indicado en el numeral 9.2.2, relativo a elementos de soporte, de la norma técnica NCh-ISO 27.002, de 2009, 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 el municipio argumenta que se realizarán las estrategias para poder mejorar la red eléctrica del proceso de mejoras, asimismo, generar los planes de contingencia ante eventos emergentes.

Al tenor de lo expuesto, y considerando que las acciones informadas aún no se concretan, se mantiene la situación objetada, por lo que ese municipio deberá acreditar las acciones referidas a la implementación de la red eléctrica y la creación de planes de contingencia, remitiendo la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

10. Deficiencia en la mantención de arquitectura tecnológica[2].

Sobre la materia, cabe indicar que, de las diligencias practicadas en terreno, el encargado de informática señaló que no se cuenta con un inventario de todos los equipos que integran la zona de servidores y comunicaciones, asimismo, como se indicó anteriormente, no cuenta con la información necesaria sobre el mantenimiento de los equipos auxiliares y no se han elaborado un plan de contingencia, según consta en acta de fiscalización de fecha 22 de noviembre de 2022.

Lo hechos antes mencionados transgreden lo dispuesto en el punto 9.2.4, sobre mantenimiento del equipamiento, de la norma técnica NCh-ISO 27.002, de 2009, que señala que el equipamiento se debería mantener adecuadamente para asegurar su continua disponibilidad e integridad.

El ente comunal, en su contestación, indica que se establecerá una política de mantenimiento de los equipos auxiliares y la elaboración de plan de contingencia ante eventos emergentes.

En razón de anterior y que las acciones informadas por el municipio aún no se concretan, se mantiene la observación, no

[2] Una arquitectura tecnológica o plataforma tecnológica, incluye el conjunto de recursos que en materia de Tecnologías de Información y Comunicaciones, TIC, (programas, soportes, archivos, datos, información, redes internas y públicas, equipos para el almacenamiento, la seguridad, el control, el tratamiento, la generación, comunicación y transmisión de datos en todos sus formatos) utilice la Municipalidad de Angol, numeral 3, “términos/definiciones”, Reglamento de Uso y Seguridad de la Plataforma Tecnológica, de la Municipalidad de Angol.

obstante el municipio deberá realizar las medidas informadas, debiendo acreditar las acciones referidas a la elaboración de la política de mantenimiento que incluya a todos los equipos que conforman su plataforma tecnológica y su plan de contingencias, remitiendo la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

11. No existe procedimiento de destrucción de información en dispositivos electrónicos.

Se advirtió que el municipio no cuenta con un procedimiento de eliminación de información sensible, en dispositivos electrónicos que son retirados de operación, lo que vulnera lo establecido en los artículos 15, letra d), sobre la clasificación, control y etiquetado de bienes, y 26, letra e), del aludido decreto N° 83, de 2004, el cual señala que se debe verificar que todos los equipos informáticos y medios digitales que sean usados en el almacenamiento y/o procesamiento de documentos electrónicos, de ser posible, sean reformateados previo a ser dados de baja.

Así también, no es armónico con lo señalado en los numerales 10.7.2 de la norma NCh-ISO 27.002, de 2009, que establece que se deberían eliminar los medios de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales.

En su respuesta, la autoridad comunal señala que se elaborará una política en relación a la destrucción de datos almacenados en discos duros y otras formas de medios electrónicos para que sean completamente ilegibles y no se puedan acceder a ellos ni utilizar con fines no autorizados.

Atendido que las acciones informadas por el municipio aún no se concretan, se mantiene la observación, por lo que esa entidad deberá concretar las medidas informadas en orden a estandarizar los procesos de eliminación de los dispositivos informáticos en la política de seguridad de la información municipal, lo que deberá ser acreditado, remitiendo la documentación pertinente ante esta Sede Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

12. Inexistencia de procedimientos formalizados de copias de seguridad y recuperación de información.

Se constató que el municipio no cuenta con un procedimiento formal que permita asegurar la operación correcta de las copias de seguridad y de la restauración de estas, lo que transgrede lo exigido en el artículo 37, letra f), del referido decreto N° 83, de 2004, asimismo, el literal 10.1.1, de la mencionada norma NCh-ISO 27.002, de 2009, que señala que los procedimientos de operación se deberían documentar, mantener y poner a disposición de todos los usuarios que los necesiten.

13. Deficiencias en validación de copias de seguridad.

El encargado de informática confirmó que el municipio, respecto de los respaldos de información, no verifica, examina y/o

comprueba que -una vez concluido dicho proceso de respaldo- dichas copias de información y sus dispositivos de almacenamientos, contengan toda la información duplicada, sino más bien, los usuarios se cercioran que esas copias contienen los datos en el momento que son utilizados, para una eventual restauración o utilización de ellos.

Lo descrito, vulnera el artículo 37, letra f) del precitado decreto N° 83, de 2004, y el punto 10.5.1, de la mencionada norma NCh-ISO 27.002, de 2009, sobre respaldo de la información, el cual dice que, se deberían hacer regularmente copias de seguridad de la información y del software y probarse regularmente acorde con la política de respaldo.

En relación a los numerales 12 y 13, precedentes, en su respuesta el alcalde manifiesta que, por una parte, se elaborará una política de copias de seguridad y recuperación de la información ante eventos emergentes, conforme a los plazos consignados en el plan y, por otra, que se instruirán realizar mejoras en relación a la verificación de las copias de seguridad, en el cual se establecerá que una vez concluido el proceso de respaldos se deberá comprobar que los estos contengan toda la información, siendo el personal informático el responsable de verificar dicha copia de archivos.

Al tenor de lo expuesto, y considerando que las acciones informadas aún no se concretan, se mantiene las situaciones objetadas, por lo que ese municipio deberá acreditar las acciones referidas, por una parte, sobre la política de copias de seguridad y recuperación de la información, y, por otra, lo referido al procedimiento de verificación de las copias de seguridad de la información, remitiendo la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

14. Ausencia de log de transacciones en las aplicaciones.

Se constató que el municipio no ha implementado un log de transacciones[3] de las bases de datos de sus sistemas, en los cuales queden contenidos los detalles de los movimientos de todas las actividades, transacciones, eventos y fallos.

Dicha situación, vulnera lo establecido en el artículo 7°, la letra d) del citado decreto N° 83, de 2004, que señala que se debe monitorear el cumplimiento de los procedimientos establecidos y revisarlos de manera de evitar incidentes de seguridad, asimismo, el artículo 23, de igual normativa, el que indica, en lo que interesa, que para reducir el riesgo de negligencia o mal uso deliberado de los sistemas, deberán aplicarse políticas de segregación de funciones e incorporar mecanismos periódicos de auditorías de la integridad de los registros de datos almacenados en documentos electrónicos.

Por último, infringe el numeral 10.10.5, de la NCh-ISO 27.002, de 2009, sobre registros de fallas, que establece, que éstas deberían ser registradas, analizadas y tomar las acciones apropiadas.

[3] Es un reporte que registra todas las actividades y las modificaciones que se realiza en un sistema.

Sobre la materia, la entidad señala que hay registros de log de transacciones, con el contenido de los detalles de los movimientos, razón por lo cual adjunta una imagendel archivo con la tabla que contiene registros sobre dichos registros de cambios de datos.

Considerando que el municipio acompañó en su respuesta los antecedentes que dan cuenta de los registros de log de transacciones, se revuelve subsanar la observación para este caso.

Sin perjuicio de lo anterior, corresponde que el municipio implemente una revisión permanente a las fallas que se identifican en el Log, registros de sus sistemas, a objeto de verificar las actividades, transacciones, eventos y fallos, que pudiesen ser sujetos de acciones que deba emprender el municipio, para que dichas situaciones no vuelvan a ocurrir.

15. Ausencia de controles en la creación de contraseñas.

Sobre el particular, se constató que la municipalidad no ha implemento un mecanismo para asegurar la seguridad y calidad de las contraseñas, situación que contraviene lo dispuesto en el artículo 37, letra g), del ya citado decreto N° 83, de 2004, el cual debe entenderse referida al capítulo 11 de la norma técnica NCh-ISO 27.002, de 2009, sobre Control de Acceso, y que, en lo que interesa, en el punto 11.3.1, denominado “uso de contraseña”, manifiesta que se debería exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas, que implica contraseñas de calidad que cumplan con una estructura determinada, como por ejemplo un largo mínimo, uso de números y letras, caracteres especiales, restricción en la reutilización, establecer períodos de vigencia, entre otros.

El ente comunal, señala que se establecerá un mecanismo o se contratará un software para el control y manejo de contraseñas, según los plazos estipulados en el plan.

En razón de anterior y que las acciones informadas por el municipio, aún no se concretan, se mantiene la observación, no obstante, el municipio deberá realizar las medidas informadas, debiendo acreditar la implementación del mecanismo para controlar la seguridad y calidad de las contraseñas que utilizan los funcionarios en los equipos o sistemas de la plataforma tecnológica del municipio, remitiendo la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

16. Inexistencia de políticas y procedimiento de acceso remoto.

Se constató que el municipio no cuenta con un documento en donde se establezca una política y procedimiento respecto al control de acceso remoto, en lo referido al uso de redes y servicios de red a las que el acceso de los funcionarios está permitido.

Lo anterior, contraviene lo establecido en el artículo 33, del mencionado decreto N° 83, de 2004, asimismo, la situación expuesta

no se ajusta a lo dispuesto en el punto 11.7, de la citada norma NCh-ISO 27.002, de 2009, la que señala que el trabajo remoto e informática móvil, requerirá una protección la cual deberá ser proporcional a los riesgos que causan estas formas específicas de trabajo. En donde, añade, se deberían considerar los riesgos de trabajar en un entorno desprotegido cuando se usa informática móvil y aplicar la protección adecuada.

La municipalidad señala que se elaborará un manual de políticas informáticas, y en ella se considerarán instrucciones sobre la materia reprochada, asimismo, se evaluará la posibilidad de comprar una licencia de un software para el acceso remoto.

En virtud que las acciones informadas por el municipio aún no se concretan, se mantiene la observación, por lo tanto esa entidad deberá emprender las medidas informadas, debiendo acreditar las medidas referidas a la confección del aludido manual de políticas que contemple la materia reprochada y, de corresponder, la implementación del software para administrar los accesos remotos, remitiendo los antecedentes pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

17. Inexistencia de una política de clasificación de información sensible.

El encargado de informática del municipio, señaló que no se realiza ningún tipo categorización para establecer que información debe o no ser protegida (encriptada), situación que no mitiga los eventuales riesgos de confidencialidad, autenticidad o integridad de la información de la entidad auditada. Lo anterior, vulnera el artículo 13, del referido decreto N° 83, de 2004, el que establece que los documentos electrónicos y sistemas informáticos deberán clasificarse y etiquetarse para indicar la necesidad, prioridad y grado de protección.

Adicionalmente, lesiona el punto 7.2, denominado “Clasificación de la información”, de la norma técnica NCh-ISO 27.002, de 2009, el cual establece que se debe asegurar que la información recibe el nivel de protección adecuado, por lo tanto, se debería clasificar para indicar la necesidad, prioridades y grado de protección esperado en el manejo de esta.

Esa entidad reconoce la situación detectada y en atención a ello, indica que se realizará una categorización de ella, asimismo, se elaborará un procedimiento para establecer que información debe o no ser protegida, encriptada, con el objeto de mitigar eventuales riesgos de confidencialidad y autenticidad.

Al tenor de lo expuesto, y considerando que las acciones informadas, aún no se concretan, se mantiene la situación objetada, por lo que ese municipio deberá acreditar las medidas referidas a la elaboración de una política de clasificación de información sensible y de los avances, respecto a su aplicabilidad, si corresponde, remitiendo la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

18. Diferencias entre activos TI y el licenciamiento de uso de software.

De la revisión efectuada a los antecedentes proporcionados por el municipio, estos permitieron advertir la inexistencia de un inventario de activos de TI, sin embargo, el profesional encargado del departamento de informática presentó un catastro -de activos TI- no oficial e incompleto, el cual detalla información de 30 equipos computacionales, de los cuales se informó la existencia de 92 licencias de paquetes de software de informática y 150 softwares de antivirus, generándose una incongruencia con respecto de lo equipos y sus respectivas licencias.

Al respecto, lo expuesto vulnera lo establecido en la letra b) del artículo 22, del citado decreto N° 83, de 2004, sobre gestión de las operaciones y las comunicaciones, sobre cumplimiento de las licencias de software y la prohibición del uso de software no autorizado, y además de lo estipulado en los artículos 19 y 20, de la ley N° 17.336, sobre Propiedad Intelectual, que disponen que nadie podrá utilizar públicamente una obra del dominio privado sin haber obtenido la autorización expresa del titular del derecho de autor, la infracción de lo dispuesto en este artículo hará incurrir al o los responsables en las sanciones civiles y penales correspondientes.

En respuesta el municipio indica que se confeccionarán por separado, los inventarios con activos TI y el de uso de software, de conformidad a los plazos estipulados en el plan.

En virtud que las acciones informadas por el municipio, aún no se concretan, se mantiene la observación, por lo tanto, la municipalidad deberá remitir el reporte que acredite las acciones informadas, sobre la confección del inventario de los bienes TI y la adquisición de las licencias faltantes de aquellos equipos que no cuentan con ellas, y su respectivo registro en dicho procedimiento de control, remitiendo la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

19. Ausencia de cláusulas de confidencialidad en servicios de software.

Sobre la materia, se constató que el servicio de arriendo de programas computacionales, en específico el sistema de gestión municipal con la empresa CASCHILE S.A, no contempla la inclusión de cláusulas de confidencialidad, advirtiéndose así la falta de acuerdos que reflejen las necesidades de protección de la información del municipio.

La situación antes expuesta vulnera lo dispuesto en la letra b), del artículo 37, del referido decreto N° 83, de 2004, sobre seguridad organizacional, en concordancia con lo señalado en el acápite 6.2.3, de la norma chilena NCh-ISO 27.002, de 2009, sobre tener en cuenta la seguridad en los acuerdos con terceras partes.

Sobre la materia, el municipio señala que en los futuros procesos de licitación se establecerán en las respectivas bases las cláusulas de confidencialidad en servicios o bien mediante requerimientos formales a

los proveedores, cometido que está establecida en el plan, el cual se confeccionó en base a la hoja de ruta ISO 27001, sobre Seguridad de la Información.

Atendido a que en su contestación, el municipio reconoce lo observado y alude a medidas que aún no se concretan, pues ellas se aplicarán en el futuro, se mantienen las situaciones objetadas, por lo tanto esa entidad deberá concretar las medidas informadas respecto a establecer en las respectivas bases de futuras licitaciones, las cláusulas de confidencialidad en servicios o bien mediante requerimientos formales a los proveedores, lo cual deberá acreditar documentadamente ante la Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

20. Inexistencia de un plan de contingencia.

Se evidenció, que la Municipalidad de Angol no ha elaborado un documento oficial que establezca un plan de contingencia, donde se detallen las acciones a seguir durante la ocurrencia de un siniestro, de modo que les permita asegurar la continuidad de operaciones críticas de dicha entidad.

Lo descrito contraviene lo establecido en la letra i), del artículo 37 del aludido decreto N° 83, de 2004, el cual establece que se aplicarán las estipulaciones del capítulo 11 de la norma NCh 2.777, en su integridad, la que debe entenderse referida al capítulo 14 de la norma NCh-ISO 27.002, de 2009, que la reemplaza, la cual señala, en el punto 14.1.3, denominado “Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información”, que se deberían desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requeridos, después de la interrupción o la falla de los procesos críticos para el negocio.

El alcalde informa que se confeccionará un documento oficial que establezca un plan de contingencias, donde se detallen las acciones a seguir durante la ocurrencia de un siniestro, de modo que permita asegurar la continuidad de las operaciones críticas del municipio.

Atendido que las acciones informadas por el municipio aún no se concretan, se mantiene la observación, por lo que esa entidad deberá materializar las medidas informadas en orden a establecer un plan de contingencias, lo que deberá ser acreditado remitiendo la documentación pertinente ante esta Sede Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

21. Ausencia de un procedimiento formal de controles de cambios.

La entidad auditada no ha definido ni aprobado políticas o normas, a través de un procedimiento formal y documentado, respecto a los procedimientos de control de cambios aplicables a sus sistemas informáticos, según lo informado por el encargado de la unidad de informática.

Lo anterior, vulnera lo establecido en el artículo 37, letra f) del decreto N° 83, de 2004, la que debe entenderse referida al

capítulo 10 de la norma técnica NCh-ISO 27.002, de 2009, que menciona, en los que nos interesa, en el punto 10.1.2, sobre gestión de cambios, que se deberían controlar los cambios en los sistemas e instalaciones de procesamiento de información, en donde, se debería considerar: a) identificación y registro de cambios significativos; b) planificación y pruebas de los cambios; c) evaluación de los impactos potenciales de tales cambios, incluyendo los impactos en la seguridad; d) procedimiento formal de aprobación para los cambios propuestos; e) comunicación de los detalles del cambio a todas las personas involucradas en los mismos; f) procedimientos de vuelta atrás (fallback), incluyendo procedimientos y responsabilidades para abortar y recuperar los cambios sin éxito y de acontecimientos imprevistos.

Además, puntualiza la referida normativa, que se deberían establecer las responsabilidades y los procedimientos formales de gestión para asegurar el control satisfactorio de todos los cambios al equipamiento, software o procedimientos, en donde, además, se debería conservar un registro de auditoría conteniendo toda la información pertinente.

Sobre este punto, el municipio indica que se establecerá un procedimiento formal, debidamente formalizado, respecto a los procedimientos de control de cambios aplicables a los sistemas informáticos y al equipamiento, software u otros del área informática.

En virtud que las acciones informadas por el municipio aún no se materializan, se mantiene la observación, por lo tanto el municipio deberá concretar las medidas informadas, en orden a elaborar un documento formal, respecto a los procedimientos de control de cambios aplicables a los sistemas informáticos y al equipamiento, software u otros del área informática, lo cual deberá acreditar documentadamente ante la Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

CONCLUSIONES

Atendidas las consideraciones expuestas durante el desarrollo del presente trabajo, la Municipalidad de Angol ha aportado antecedentes de las situaciones planteadas en el preinforme de observaciones N° 927, de 2022, de esta Contraloría Regional.

En relación al numeral 14, ausencia de log de transacciones en las aplicaciones, se subsana en atención a los argumentos y antecedentes aportados.

Respecto de aquellas observaciones que se mantienen, se deberán adoptar las medidas pertinentes con el objeto de dar estricto cumplimiento a las normas legales y reglamentarias que las rigen, entre las cuales se estima necesario, a lo menos, considerar las siguientes:

1. En relación al numeral 1.1, ausencia de evaluación de riesgos de seguridad de la información (C), ese municipio deberá remitir el reporte con los resultados de la aplicación de la evaluación de los riesgos de seguridad de la información, en un plazo de 60 días hábiles en el Sistema de

Seguimiento y Apoyo CGR, a contar de la recepción del presente informe, instancia en la que se evaluará la efectividad de lo obrado.

En el numeral 1.2, ausencia de cláusulas de verificación sobre controles de acceso, respaldo de datos, continuidad de negocio y niveles de servicios, en prestaciones contratadas (C), la entidad municipal deberá hacer efectiva las medidas informadas, esto es, requerir en los futuros procesos de licitación o mediante peticiones formales a los proveedores establecidos, según se encuentra planificado en el plan adjunto, a fin de evitar de que dichas situaciones se repitan en el futuro, lo cual deberá acreditar documentadamente ante la Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

Asimismo, es necesario que el referido procedimiento se mantenga en el tiempo a fin de dar cumplimiento a lo establecido a lo establecido en los artículos 11 y 22 de la citada ley N° 19.886 y su reglamento aprobado por el decreto N° 250, de 2004, respectivamente.

2. Respecto al numeral 2, listado de funcionarios desvinculados y cambiados de funciones no puestos a disposición para el examen (C), esa entidad deberá establecer en el reglamento de uso y seguridad de la plataforma tecnológica la periodicidad de revisión y actualización o si se producen cambios significativos de la información de dichas plataformas, para asegurar su conveniencia, suficiencia, y eficacias continuas, lo que tendrá que informar el cumplimiento de lo indicado, en un plazo de 60 días hábiles en el Sistema de Seguimiento y Apoyo CGR, a contar de la recepción del presente informe.

3. Luego, en cuanto a lo consignado en el numeral 3, reglamento no establece la periodicidad de revisión (C), el municipio deberá concretar las medidas informadas, en orden a establecer en el referido documento la periodicidad de revisión y actualizaciones cuando se producen cambios significativos, de la información de dichas plataformas, para asegurar su conveniencia, suficiencia, y eficacias continuas, lo que deberá ser acreditado en el plazo de 60 días hábiles, contado desde la entrega del presente informe.

4. En lo concerniente a los numerales 4, inexistencia de un encargado de seguridad de la información (C) y 5, inexistencia de un comité de seguridad de la información (C), la entidad edilicia deberá arbitrar las medidas tendientes a regularizar dichas situaciones, debiendo acreditar las acciones informadas referidas al nombramiento del funcionario en calidad de encargado de seguridad, procurando que exista un control de oposición de funciones o de segregación de funciones en las labores del referido cargo. Del mismo modo, deberá acreditar las acciones referidas a la creación de un comité de seguridad de información. Para ambos casos, deberá remitir la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contados desde la recepción del presente informe.

5. Para lo representado en el numeral 6, ausencia de un inventario con el detalle de los activos de tecnologías de información, TI, (C), el municipio deberá remitir un informe con un avance de los resultados obtenidos de la actualización del inventario informático municipal, el cual incluya no

solo los activos físicos TI, sino que también los activos de software, en un plazo de 60 días hábiles a contar de la recepción del presente informe, instancia en la que se evaluará la efectividad de lo realizado.

6. Sobre el numeral 7, inexistencia de seguridad física para los servidores (C) y 8, ausencia de controles ambientales para la zona de servidores (C), la municipalidad deberá emprender las medidas informadas, debiendo acreditar, por una parte, sobre la segmentación de las dependencias de los servidores y las aéreas que correspondan y, por otra, sobre la instalación de los equipos de climatización, a fin de generar las mejoraras informadas, lo que deberá ser acreditado en el plazo de 60 días hábiles, contado desde la entrega del presente informe.

7. En cuanto a lo objetado en el numeral 9, deficiencia en suministro eléctrico para los servidores (C), el municipio deberá acreditar las acciones referidas a la implementación de la red eléctrica y la creación de planes de contingencia, remitiendo la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

8. En lo que respecta al numeral 10, deficiencia en la mantención de arquitectura tecnológica (C), el municipio deberá realizar las medidas informadas, debiendo acreditar las acciones referidas a la elaboración de la política de mantenimiento que incluya a todos los equipos que conforman su plataforma tecnológica y su plan de contingencias, remitiendo la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

9. En relación al numeral 11, no existe procedimiento de destrucción de información en dispositivos electrónicos (C), esa entidad deberá concretar las medidas informadas en orden a estandarizar los procesos de eliminación de los dispositivos informáticos en la política de seguridad de la información municipal, lo que deberá ser acreditado remitiendo la documentación pertinente ante esta Sede Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

10. En lo que concierne a los numerales 12, inexistencia de procedimientos formalizados de copias de seguridad y recuperación de información (C) y 13, deficiencias en validación de copias de seguridad (C), ese municipio deberá concretar las medidas informadas, para ello le corresponderá acreditar, por una parte, sobre la política de copias de seguridad y recuperación de la información, y, por otra, lo referido al procedimiento de verificación de las copias de seguridad de la información, remitiendo la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

11. Luego, en cuanto a lo reprochado en el numeral 15, ausencia de controles en la creación de contraseñas (C), la entidad fiscalizada deberá realizar las medidas informadas, debiendo acreditar la implementación del mecanismo para controlar la seguridad y calidad de las contraseñas que utilizan los funcionarios en los equipos o sistemas de la plataforma

tecnológica del municipio, remitiendo la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

12. En lo concerniente al numeral 16, inexistencia de políticas y procedimientos de acceso remoto (C), la municipalidad deberá realizar las medidas informadas, debiendo acreditar las acciones referidas a la confección del aludido manual de políticas que contemple la materia reprochada y, de corresponder, la implementación del software para administrar los accesos remotos, remitiendo los antecedentes pertinentes ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

13. Para lo representado en el numeral 17, inexistencia de una política de clasificación de información sensible (C), ese municipio deberá acreditar las medidas referidas a la elaboración de una política de clasificación de información sensible y de los avances respecto a su aplicabilidad, si corresponde, remitiendo la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

14. Sobre el numeral 18, diferencia entre activo TI y el licenciamiento de uso de software (C), la municipalidad deberá remitir el reporte que acredite las acciones informadas, sobre la confección del inventario de los bienes TI y la adquisición de las licencias faltantes de aquellos equipos que no cuentan con ellas, y su respectivo registro en dicho procedimiento de control, remitiendo la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

15. En cuanto a lo objetado en el numeral 19, ausencia de cláusulas de confidencialidad en servicios de software (C), esa entidad deberá concretar las medidas informadas respecto a establecer en las respectivas bases de futuras licitaciones, las cláusulas de confidencialidad en servicios o bien mediante requerimientos formales a los proveedores, lo cual deberá acreditar documentadamente ante la Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

16. En lo que respecta al numeral 20, inexistencia de un plan de contingencia (C), esa entidad deberá materializar las medidas informadas en orden a establecer un plan de contingencias, lo que deberá ser acreditado remitiendo la documentación pertinente ante esta Sede Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

17. En relación al numeral 21, ausencia de un procedimiento formal de controles de cambios (C), el municipio deberá concretar las medidas informadas, en orden a elaborar un documento formal, respecto a los procedimientos de control de cambios aplicables a los sistemas informáticos y al equipamiento, software u otros del área informática, lo cual deberá acreditar documentadamente ante la Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.

Finalmente, en lo que dice relación con cada una de las conclusiones catalogadas como compleja (C), de acuerdo al formato

adjunto en el anexo N° 2, las medidas que al efecto implemente el municipio, 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 Órgano Contralor, en el plazo que se expone en cada caso, contado a partir de la recepción del presente informe.

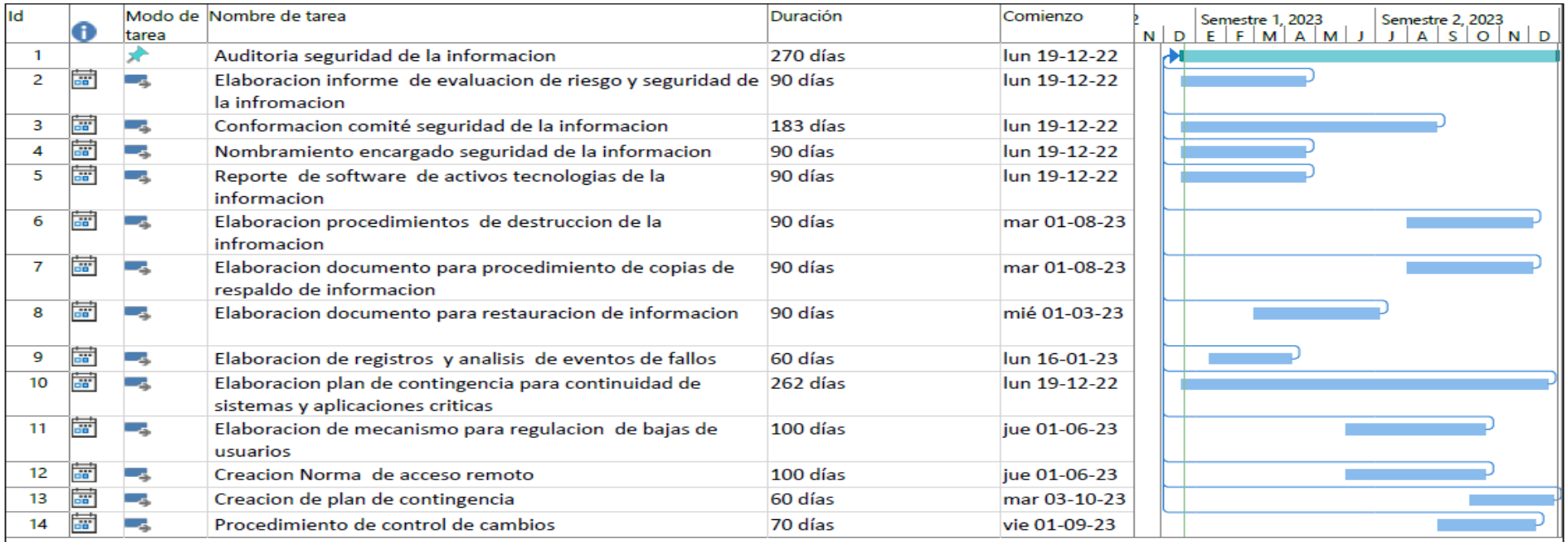
Remítase el presente informe al Alcalde, Secretario Municipal y al Director de Control Interno, todos de la Municipalidad de Angol.

Saluda atentamente a Ud.,

Firmado electrónicamente por:	
Nombre:	CARLOS BILBAO FUENTES
Cargo:	Jefe de Unidad de Control Externo
Fecha:	28/12/2022

Anexo N° 1: “Carta Gantt auditoría de seguridad de la información”

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo
1		Auditoria seguridad de la informacion	270 días	lun 19-12-22
2		Elaboracion informe de evaluacion de riesgo y seguridad de la infromacion	90 días	lun 19-12-22
3		Conformacion comité seguridad de la informacion	183 días	lun 19-12-22
4		Nombramiento encargado seguridad de la informacion	90 días	lun 19-12-22
5		Reporte de software de activos tecnologias de la informacion	90 días	lun 19-12-22
6		Elaboracion procedimientos de destruccion de la infromacion	90 días	mar 01-08-23
7		Elaboracion documento para procedimiento de copias de respaldo de informacion	90 días	mar 01-08-23
8		Elaboracion documento para restauracion de informacion	90 días	mié 01-03-23
9		Elaboracion de registros y analisis de eventos de fallos	60 días	lun 16-01-23
10		Elaboracion plan de contingencia para continuidad de sistemas y aplicaciones criticas	262 días	lun 19-12-22
11		Elaboracion de mecanismo para regulacion de bajas de usuarios	100 días	jue 01-06-23
12		Creacion Norma de acceso remoto	100 días	jue 01-06-23
13		Creacion de plan de contingencia	60 días	mar 03-10-23
14		Procedimiento de control de cambios	70 días	vie 01-09-23



Página 1

Fuente: planificación elaborada por la Municipalidad de Angol y acompañada en su oficio de respuesta N° 2.764/575, de 19 de diciembre de 2022.

Anexo N° 2: Estado de observaciones de informe final de auditoría N° 927, de 2022, Municipalidad de Angol.

Nº DE OBSERVACIÓN Y ACÁPITE	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN EFECTUADA 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
1.1 del Acápite I, Aspectos de Control Interno.	Ausencia de evaluación de riesgos de seguridad de la información.	C: compleja.	El municipio deberá remitir el reporte con los resultados de la aplicación de la evaluación de los riesgos de seguridad de la información, en un plazo de 60 días hábiles en el Sistema de Seguimiento y Apoyo CGR, a contar de la recepción del presente informe, instancia en la que se evaluará la efectividad de lo obrado.			
1.2 del Acápite I, Aspectos de Control Interno.	Ausencia de cláusulas de verificación sobre controles de acceso, respaldo de datos, continuidad de negocio y niveles de servicios, en prestaciones contratados.	C: compleja.	La entidad municipal deberá hacer efectiva las medidas informadas, esto es, requerir en los futuros procesos de licitación o mediante peticiones formales a los proveedores establecidos, según se encuentra planificado en el plan adjunto, a fin de evitar de que dichas situaciones se repitan en el futuro, lo cual deberá acreditar documentadamente ante la Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.			
2 del Acápite II, Examen de la Materia Auditada.	Listado de funcionarios desvinculados y cambiados de funciones no puestos a disposición para el examen.	C: compleja.	Esa entidad deberá comunicar sobre la efectividad o no de las medidas informadas, referidas al procedimiento de verificación de eliminación de perfiles de los funcionarios desvinculados y/o cambiados de funciones, a fin de generar las mejoraras informadas, lo que deberá ser acreditado en el plazo de 60 días hábiles, contado desde la entrega del presente informe.			
3 del Acápite II, Examen de la Materia Auditada.	Reglamento no establece la periodicidad de revisión.	C: compleja.	El municipio deberá establecer en el reglamento de uso y seguridad de la plataforma tecnológica la periodicidad de revisión y actualización o si se producen cambios significativos, de la información de dichas plataformas, para asegurar su			

Nº DE OBSERVACIÓN Y ACÁPITE	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN EFECTUADA 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
			conveniencia, suficiencia, y eficacias continuas, lo que tendrá que informar el cumplimiento de lo indicado, en un plazo de 60 días hábiles en el Sistema de Seguimiento y Apoyo CGR, a contar de la recepción del presente informe.			
4 del Acápite II, Examen de la Materia Auditada.	Inexistencia de un encargado de seguridad de la información.	C: compleja.	La entidad edilicia deberá arbitrar las medidas tendientes a regularizar dichas situaciones, debiendo acreditar las acciones informadas referidas al nombramiento del funcionario en calidad de encargado de seguridad, procurando que exista un control de oposición de funciones o de segregación de funciones en las labores del referido cargo, del mismo modo, deberá acreditar las acciones referidas a la creación de un comité de seguridad de información. Para ambos casos deberá remitir la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contados desde la recepción del presente informe.			
5 del Acápite II, Examen de la Materia Auditada.	Inexistencia de un comité de seguridad de la información.	C: compleja.				
6 del Acápite II, Examen de la Materia Auditada.	Ausencia de un inventario con el detalle de los activos de tecnologías de información, TI.	C: compleja.	El municipio deberá remitir un informe con un avance de los resultados obtenidos de la actualización del inventario informático municipal, el cual incluya no solo los activos físicos TI, sino que también los activos de software, en un plazo de 60 días hábiles a contar de la recepción del presente informe, instancia en la que se evaluará la efectividad de lo realizado.			
7 del Acápite II, Examen de la Materia Auditada.	Inexistencia de seguridad física para los servidores.	C: compleja.	La municipalidad deberá emprender las medidas informadas, debiendo acreditar, por una parte, sobre la segmentación de las dependencias de los servidores y las aéreas			

Nº DE OBSERVACIÓN Y ACÁPITE	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN EFECTUADA 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
8 del Acápite II, Examen de la Materia Auditada.	Ausencia de controles ambientales para la zona de servidores.	C: compleja.	que correspondan y, por otra, sobre la instalación de los equipos de climatización, a fin de generar las mejoraras informadas, lo que deberá ser acreditado en el plazo de 60 días hábiles, contado desde la entrega del presente informe.			
9 del Acápite II, Examen de la Materia Auditada.	Deficiencia en suministro eléctrico para los servidores.	C: compleja.	El municipio deberá acreditar las acciones referidas a la implementación de la red eléctrica y la creación de planes de contingencia, remitiendo la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.			
10 del Acápite II, Examen de la Materia Auditada.	Deficiencia en la mantención de arquitectura tecnológica	C: compleja.	El municipio deberá realizar las medidas informadas, debiendo acreditar las acciones referidas a la elaboración de la política de mantenimiento que incluya a todos los equipos que conforman su plataforma tecnológica y su plan de contingencias, remitiendo la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.			
11 del Acápite II, Examen de la Materia Auditada.	No existe procedimiento de destrucción de información en dispositivos electrónicos.	C: compleja.	Esa entidad deberá concretar las medidas informadas en orden a estandarizar los procesos de eliminación de los dispositivos informáticos en la política de seguridad de la información municipal, lo que deberá ser acreditado, remitiendo la documentación pertinente ante esta Sede Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.			

Nº DE OBSERVACIÓN Y ACÁPITE	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN EFECTUADA 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
12 del Acápite II, Examen de la Materia Auditada.	Inexistencia de procedimientos formalizados de copias de seguridad y recuperación de información.	C: compleja.	Ese municipio deberá concretar las medidas informadas, para ello le corresponderá acreditar, por una parte, sobre la política de copias de seguridad y recuperación de la información, y, por otra parte, lo referido al procedimiento de verificación de las copias de seguridad de la información, remitiendo la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.			
13 del Acápite II, Examen de la Materia Auditada.	Deficiencias en validación de copias de seguridad.	C: compleja.				
15 del Acápite II, Examen de la Materia Auditada.	Ausencia de controles en la creación de contraseñas.	C: compleja.	La entidad fiscalizada deberá realizar las medidas informadas, debiendo acreditar la implementación del mecanismo para controlar la seguridad y calidad de las contraseñas que utilizan los funcionarios en los equipos o sistemas de la plataforma tecnológica del municipio, remitiendo la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.			
16 del Acápite II, Examen de la Materia Auditada.	Inexistencia de políticas y procedimiento de acceso remoto.	C: compleja.	La municipalidad deberá realizar las medidas informadas, debiendo acreditar las acciones referidas a la confección del aludido manual de políticas que contemple la materia reprochada y, de corresponder, la implementación del software para administrar los accesos remotos, remitiendo los antecedentes pertinentes ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.			
17 del Acápite II, Examen de la Materia Auditada.	Inexistencia de una política de clasificación de información sensible.	C: compleja.	Ese municipio deberá acreditar las medidas referidas a la elaboración de una política de clasificación de información sensible y de los avances, respecto, a su aplicabilidad, si corresponde, remitiendo la documentación			

Nº DE OBSERVACIÓN Y ACÁPITE	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN EFECTUADA 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
			pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.			
18 del Acápite II, Examen de la Materia Auditada.	Diferencias entre activos TI y el licenciamiento de uso de software.	C: compleja.	La municipalidad deberá remitir el reporte que acredite las acciones informadas, sobre la confección del inventario de los bienes TI y la adquisición de las licencias faltantes de aquellos equipos que no cuentan con ellas, y su respectivo registro en dicho procedimiento de control, remitiendo la documentación pertinente ante esta Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.			
19 del Acápite II, Examen de la Materia Auditada.	Ausencia de cláusulas de confidencialidad en servicios de software.	C: compleja.	Esa entidad deberá concretar las medidas informadas respecto a establecer en las respectivas bases de futuras licitaciones, las cláusulas de confidencialidad en servicios o bien mediante requerimientos formales a los proveedores, lo cual deberá acreditar documentadamente ante la Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.			
20 del Acápite II, Examen de la Materia Auditada.	Inexistencia de un plan de contingencia.	C: compleja.	Esa entidad deberá materializar las medidas informadas en orden a establecer un plan de contingencias, lo que deberá ser acreditado, remitiendo la documentación pertinente ante esta Sede Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.			
21 del Acápite II, Examen de la Materia Auditada.	Ausencia de un procedimiento formal de controles de cambios.	C: compleja.	El municipio deberá concretar las medidas informadas, en orden a elaborar un documento formal, respecto a los procedimientos de control de cambios aplicables a los sistemas informáticos y al equipamiento, software u otros del área			

Nº DE OBSERVACIÓN Y ACÁPITE	MATERIA DE LA OBSERVACIÓN	NIVEL DE COMPLEJIDAD	REQUERIMIENTO PARA SUBSANAR LA OBSERVACIÓN EFECTUADA 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
			informática, lo cual deberá acreditar documentadamente ante la Contraloría Regional, en el término de 60 días hábiles, contado desde la recepción del presente informe.			

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

REMITE INFORME FINAL DE AUDITORÍA N° 927, DE 2022, EFECTUADA EN LA MUNICIPALIDAD DE ANGOL.

TEMUCO,

Se remite, para su conocimiento y fines pertinentes, el informe final Nº 927, de 2022, sobre auditoría al macroproceso de Tecnologías de la Información, TI, con la finalidad de revisar y evaluar el nivel de seguridad informática implementado por la Municipalidad de Angol, 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 anotado decreto N° 83, de 2004, en el periodo comprendido entre 1 de marzo de 2021 al 30 de noviembre de 2022.

Finalmente, cabe recordar que los datos personales, información personal y datos sensibles contenidos en el Informe 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
DE LA MUNICIPALIDAD DE ANGOL
PRESENTE

DISTRIBUCION:
- Unidad de Seguimiento y Apoyo al Cumplimiento de esta Sede de Control

Firmado electrónicamente por:	
Nombre	MARCELLO LIMONE MUÑOZ
Cargo	Contralor Regional
Fecha firma	28/12/2022
Código validación	YcK5S5A3h
URL validación	https://www.contraloria.cl/validardocumentos

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

REMITE INFORME FINAL DE AUDITORÍA N° 927, DE 2022, EFECTUADA EN LA MUNICIPALIDAD DE ANGOL.

TEMUCO,

Se remite, para su conocimiento y fines pertinentes, el informe final Nº 927, de 2022, sobre auditoría al macroproceso de Tecnologías de la Información, TI, con la finalidad de revisar y evaluar el nivel de seguridad informática implementado por la Municipalidad de Angol, 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 anotado decreto N° 83, de 2004, en el periodo comprendido entre 1 de marzo de 2021 al 30 de noviembre de 2022, 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 este organismo colegiado entregándole copia del mismo.

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

Finalmente, cabe recordar que los datos personales, información personal y datos sensibles contenidos en el Informe 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.,

A LA SEÑORA
SECRETARIA MUNICIPAL (s)
DE LA MUNICIPALIDAD DE ANGOL
PRESENTE

Firmado electrónicamente por:	
Nombre	MARCELLO LIMONE MUÑOZ
Cargo	Contralor Regional
Fecha firma	28/12/2022
Código validación	YcK5S5A1N
URL validación	https://www.contraloria.cl/validardocumentos

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

REMITE INFORME FINAL DE AUDITORÍA N° 927, DE 2022, EFECTUADA EN LA MUNICIPALIDAD DE ANGOL.

TEMUCO,

Se remite, para su conocimiento y fines pertinentes, el informe final Nº 927, de 2022, sobre auditoría al macroproceso de Tecnologías de la Información, TI, con la finalidad de revisar y evaluar el nivel de seguridad informática implementado por la Municipalidad de Angol, 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 anotado decreto N° 83, de 2004, en el periodo comprendido entre 1 de marzo de 2021 al 30 de noviembre de 2022.

Finalmente, cabe recordar que los datos personales, información personal y datos sensibles contenidos en el Informe 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
DIRECTOR DE CONTROL INTERNO
DE LA MUNICIPALIDAD DE ANGOL
PRESENTE

Firmado electrónicamente por:	
Nombre	MARCELLO LIMONE MUÑOZ
Cargo	Contralor Regional
Fecha firma	28/12/2022
Código validación	YcK5S5AnO
URL validación	https://www.contraloria.cl/validardocumentos