INFORME Nº 07

Constitución, 14 de febrero 2024.-

Ref. : Auditoría a las Tecnologías de la Información y Comunicaciones Informe Final N° 19/2019.

De : **DIRECTOR DE CONTROL INTERNO**

A : **SECPLAN.-**

Junto con saludarles, y en virtud a lo previsto en el artículo N° 29, de la Ley N° 18.695.- Orgánica Constitucional de Municipalidades, y la Circular N° 14.100.- de la Contraloría General de la República, en cuanto a las observaciones catalogadas como (MC) mediamente complejas y (LC) levemente complejas, su cumplimiento será fiscalizado por esta Dirección de Control.- me permito realizar nuevamente un re-seguimiento, respecto al informe Final sobre Tecnologías de la Información y Comunicaciones, TIC, realizada por la contraloría según el Informe Final N° 19/2019 del 3 de Julio de 2019., el cual aún se mantiene pendientes siete observaciones en el sistema de seguimiento de auditorías en el portal administrado por ese organismo de Control.

Esta Dirección de control interno, mediante documentos que se mencionan a continuación, informo a los departamentos involucrados en la auditoria sobre los resultados del informe final, solicitando subsanar las observaciones, remitiendo las respuestas a los reparos efectuados, no obstante, no se recibió respuesta, oficial.

- Informe N°10 del 25/07/19 "Seguimiento a informe final n°19/2019 Auditoria Tecnología de Información"
- Memorándum N°294 del 30/07/19 "Observación al contrato denominado "Servicios de Mantención Preventiva de Datos de Seguridad y Red Computacional ID N°2827-7-LE19"
- Memorándum N°324 del 19/08/19 "Observación al contrato denominado "Servicios de Mantención Preventiva de Datos de Seguridad y Red Computacional ID N°2827-7-LE19"
- Informe N°12 del 23/08/19 "Seguimiento a informe final n°19/2019 Auditoria Tecnología de Información"
- Informe N°13 del 16/10/19 "Seguimiento a informe final n°19/2019 Auditoria Tecnología de Información"
- Informe N°14 del 16/10/19 "Seguimiento a informe final n°19/2019 Auditoria Tecnología de Información"
- Informe N° 17 de 23/12/2020 "Auditoria de Seguimiento a las Tecnología de Información, sobre Informe Final N° 19/2019 de Contraloría Regional."
- Informe N° 15 de 23/08/2021 "Re-Seguimiento a las Tecnología de Información, sobre Informe Final N° 19/2019 de Contraloría Regional
- Informe N° 04 de 08/04/2022 "Re-Seguimiento a las Tecnología de Información, sobre Informe Final N° 19/2019 de Contraloría Regional

En relación con las observaciones que aun se mantienen pendientes, hoy en día existe el Departamento de Informática de la I. Municipalidad, conformado en primera instancia mediante Decreto exento N°2633/Q del 19 de mayo del 2023 y posteriormente con el Decreto Exento N°2857/N del 06 de junio de 2023 por el cual se destinaron los funcionarios a dicho departamento. Dichas observaciones se señalan a continuación:

OBSERVACIONES PENDIENTES:

Número de Observación en Informe: Examen de la Materia Auditada - Acápite II, N°5
Se constató que ese municipio no posee un procedimiento de revisión a intervalos regulares, por ejemplo, cada seis meses, y luego de cualquier cambio, tal como una promoción, una degradación, o terminación del empleo, de los permisos de acceso de los usuarios que incluya el registro de fechas y encargado de la revisión, infringiendo lo prescrito en la letra g), del artículo 37, del decreto N° 83, de 2004, en concordancia con el numeral 11.2.1, sobre identificación única de usuarios, de la normativa técnica NCh-ISO 27.002, de 2009.

La entidad edilicia deberá velar por la concreción de lo comunicado en el cuerpo del presente informe.

Número de Observación en Informe: Examen de la Materia Auditada - Acápite II,N°1.1;1.2

1.1. Se detectó el uso de contraseñas con una longitud inferior a 8 caracteres, no alfanuméricos y reutilizables, lo que no se ajusta a los requisitos detallados en el artículo 28, letra g), y 37, letra g) del ya aludido decreto N° 83, de 2004, entre los cuales se encuentran que deben tener una longitud mínima de 8 caracteres, sean fáciles de recordar, contengan letras, mayúsculas, dígitos y caracteres de puntuación; no estén basados en cosas obvias o de fácil deducción a partir de datos relacionados con la persona, estén libres de caracteres idénticos consecutivos o grupos completamente numéricos o alfabéticos, y no sean palabras de diccionario o nombres comunes.

Al respecto, la letra g), del artículo 37, menciona que se aplicarán las normas del capítulo 9, de la ,NCh 2.777, la que debe entenderse referida al punto 11.3 de la NCh-ISO 27.002, de 2009, que reemplaza la primera, donde

se manifiesta que se debe prevenir el acceso de usuarios no autorizados, y el robo o compromiso de la información y de las instalaciones de procesamiento de datos, exigiendo a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas.

1.2. Se comprobó que los sistemas que mantiene ese municipio no se encuentran configurados para solicitar el cambio de la contraseña al ingresar por primera vez, lo que incumple lo establecido en la letra j), del artículo 28, del decreto N° 83, de 2004, la cual dispone la indicación de cambiar el identificador temporal al iniciar la primera sesión, en concordancia con el acápite 11.2.3, letra b), de la NCh-ISO N° 27.002, de 2009.

Al respecto, es necesario recordar que las contraseñas son el mecanismo de entrada a los sistemas informáticos, por lo que, una configuración básica de las mismas podría facilitar el acceso a un intruso o atacante de los datos, comprometiendo la integridad, privacidad y confidencialidad de la información que se tiene guardada en el sistema.

Ese municipio tendrá que adoptar las medidas tendientes a asegurar la concreción de lo informado.

Número de Observación en Informe: Examen de la Materia Auditada - Acápite II, N° 4

Se verificó que la Municipalidad de Constitución no posee una política de segregación de funciones en sus sistemas informáticos, considerando que cada cuenta debe estar asociada a las labores que cumple el funcionario.

Lo expuesto contraviene lo establecido en el artículo 23 del decreto N° 83, de 2004 y el numeral 10.1.3 de la NCh-ISO N° 27.002, de 2009, el cual prevé que se deben segregar las tareas y áreas de responsabilidad para reducir la oportunidad de modificación no autorizada o no intencional, o el uso inadecuado de la información. Asimismo, la iniciación de una transacción se debe separar de su autorización.

Asimismo, lo indicado no armoniza con el numeral 54 de la resolución exenta N° 1.485, de 1996, de este Órgano Contralor, que establece que las tareas y responsabilidades principales ligadas a la autorización, tratamiento, registro y revisión de las transacciones y hechos deben ser asignadas a personas diferentes.

Número de Observación en Informe: Examen de la Materia Auditada - Acápite II, N| 8.1

De las indagaciones realizadas, se constató que la Municipalidad de Constitución no cuenta con un documento debidamente formalizado que fije un marco de gestión de la seguridad de la información, lo que fue confirmado por don Luis Ilufi Vásquez, Director de Administración y Finanzas de esa entidad.

Lo expuesto no se aviene con lo prescrito en el artículo 37, letra b), del decreto N° 83, de 2004, sobre la seguridad organizacional, que señala que se aplicará la sección 4.1, del capítulo 4 de la norma NCh 2.777, la que se debe entender referida al numeral 6.1, de la mencionada norma NCh-ISO 27.002, de 2009, que dispone 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.

Número de Observación en Informe: Examen de la Materia Auditada - Acápite II, N° 2.3

La Municipalidad de Constitución no cuenta con un procedimiento que permita eliminar o bloquear inmediatamente los derechos de acceso a los funcionarios, cuando éstos cambian de función o dejan de prestar servicios en ella, lo que fue confirmado por el Director de Administración y Finanzas de esa entidad edilicia.

Lo indicado, no se ajusta a lo dispuesto en el aludido artículo 37, letra g), del decreto N° 83, de 2004, que dispone que se aplicarán las normas del capítulo 9 de la NCh 2.777, que debe entenderse referida al punto 11.1, de la citada norma NCh-ISO 27.002, de 2009, que señala que los accesos a la información, a las instalaciones de procesamiento de la información y a procesos del negocio deberían ser controlados sobre la base de requisitos del negocio y seguridad.

Esa entidad tendrá que arbitrar las medidas necesarias a fin de contar con un procedimiento que permita eliminar o bloquear inmediatamente los derechos de acceso a los funcionarios, cuando éstos cambian de función o dejan de prestar servicios en ella, en concordancia con lo establecido en el artículo 37, letra g), del decreto N° 83, de 2004.

Número de Observación en Informe: Examen de la Materia Auditada - Acápite II, N° 8.2

Sobre el particular, se constató que esa entidad edilicia no cuenta con una política de seguridad de la información, lo que no armoniza con lo indicado en al artículo 11 del 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 el interés en el fomento y desarrollo de una cultura de seguridad institucional.

En su contestación, el jefe comunal señala que se está elaborando un documento que establezca las políticas de seguridad de la información, acceso a los sistemas y protección de redes, el que será enviado a esta Contraloría Regional cuando sea formalizado mediante el acto administrativo respectivo.

Número de Observación en Informe: Examen de la Materia Auditada - Acápite II, N° 2.1

Se verificó que ese municipio no ha nombrado a un encargado de seguridad de la información ni tampoco ha constituido un comité de seguridad, lo que fue confirmado por don Luis Ilufi Vásquez, Director de Administración y Finanzas, por medio de certificado N° 299, de 2018, vulnerándose con ello lo exigido en los artículos 12 y 37, letra b), del decreto N° 83, de 2004, del MINSEGPRES.

En efecto, el mencionado artículo 12 señala que cada organismo regido por esta norma 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 y por su parte, la letra b), del artículo 37, indica que se aplicará la sección 4.1, del capítulo 4 de la norma NCh 2.777, la que debe entenderse referida al numeral 6.1, de la mencionada norma NCh-ISO 27.002, de 2009, que manifiesta en lo que importa, que se debe establecer un marco de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

Al respecto, el acápite 6.1.1, de esta última norma, indica 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. Asimismo, el acápite 6.1:2, señala 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.

Dicha respuesta debe venir acompañada con las pruebas sustantivas necesarias que permitan verificar la realización de dichas acciones

Es todo cuanto puedo informar, quedando a vuestra disposición para responder cualquier duda, se despide de Ud.,

I. MUNICIPALIDAD DE CONSTITUCION
CONTROL INTERNO
CONSTITUCION

CESAR ARELLANO SEPÚLVEDA
DIRECTOR DE CONTROL INTERNO
I. MUNICIPALIDAD DE CONSTITUCIÓN

Distribución:

Secretaria de Planificación
C.c Alcalde
C.c. Secretaria Municipal
C.c. Administración
C.c. Asesoría Jurídica
C.c. Depto. informática
C.c. Archivo Control Interno
CAS/vcr.-