MUNICIPALIDAD DE SAN CARLOS,
SECRETARIA DEL CONCEJO MUNICIPAL
APDO 13-4.400 CIUDAD QUESADA, SAN CARLOS
TEL. 24-01-09-15 / 24-01-09-16 FAX 24-01-09-75

ACTA 72
SECRETARIA MUNICIPAL
CIUDAD QUESADA

ACTA NÚMERO SETENTA Y DOS DE LA SESIÓN EXTRAORDINARIA CELEBRADA POR EL CONCEJO MUNICIPAL DE SAN CARLOS, EL JUEVES DIEZ DE DICIEMBRE DEL DOS MIL NUEVE, A LAS CATORCE HORAS EN EL SALON DE SESIONES DE LA MUNICIPALIDAD DE SAN CARLOS.--

CAPITULO I. ASISTENCIA.--

MIEMBROS PRESENTES:

REGIDORES PROPIETARIOS, SEÑORES (AS): Gerardo Salas Lizano, Presidente Municipal, Tito Antonio Guerrero Sánchez, Ligia María Rodríguez Villalobos, María Marcela Céspedes Rojas, Teresita Quirós Gutiérrez, Ada Luz Chavarría Benavides, Dora Hidalgo Alfaro, Luis Evelio Segura Morales, Ricardo Antonio Rodríguez Delgado.--

REGIDORES SUPLENTES, SEÑORES (AS): Dora Alicia Araya Saborío, Norma Alicia Quirós Arce, Carlos Fernando Corella Chávez.--

SÍNDICOS PROPIETARIOS, SEÑORES (AS): María Leticia Navarro González, María Estilita Vásquez Vásquez, Edgar Chacón Pérez, Eladio Rojas Soto, Efrén Zúñiga Pérez, Magdalia Salazar Acosta c.c. Margalida, Margarita Durán Acuña, Auristela Saborío Arias.--

SÍNDICOS SUPLENTES, SEÑORES (AS): María Mayela Rojas Alvarado, Gisela Rodríguez Rodríguez.--

MIEMBROS AUSENTES
(SIN EXCUSA)

Adolfo Berrocal Mora, Viria Salas Zamora, Javier Armando Picado Arce, Oliver Alpízar Salas, Antonio Jiménez Alvarado, Carlos Luis Jarquín Sáenz, Judith María Arce Gómez, Nehismy Fabiola Ramos Alvarado, Idaly Solórzano Jiménez, Floribeth Jiménez Carballo, Ana Ruth Briceño Ugalde, María Adilia Rodríguez Barquero cc. Maridilia, Sady Cecilia Solórzano Salazar.-

MIEMBROS AUSENTES
(CON EXCUSA)

Ana Leticia Estrada Vargas (comisión), Edgar Rodríguez Alvarado (comisión), Aracely Segura Retana (comisión), Rafael María Rojas Quesada (comisión), Evaristo Arce Hernández (comisión), Carlos Eduardo Campos Araya (comisión), Edwin Rojas Castro (comisión), Omer Salas Vargas (comisión), José Antonio Acuña Salas (comisión).--

CAPITULO II. LECTURA DE LA AGENDA.--

ARTÍCULO No. 01. Lectura de la Agenda.--

El señor Presidente Municipal, Gerardo Salas Lizano, procede a dar lectura a la Agenda, la cual fue aprobada por unanimidad de la siguiente manera:

1.- Comprobación del Quórum.

2.- Lectura de la Agenda, aprobada mediante artículo No. 18, Acta No. 71, de la Sesión Ordinaria celebrada el lunes 07 de diciembre del 2009, en el Salón de Sesiones de la Municipalidad de San Carlos.-

PUNTO A TRATAR:

- Presentación del informe sobre los resultados de la Auditoría Interna con relación a la seguridad del área de Tecnologías de Información de la Municipalidad de San Carlos.

CAPITULO III. ATENCION A LA ADMINISTRACION MUNICIPAL.--

ARTÍCULO No. 02. Presentación del informe sobre los resultados de la Auditoría Interna con relación a la seguridad del área de Tecnologías de Información de la Municipalidad de San Carlos..--

La Ingeniera Tracy Delgado Zamora, encargada de la Auditoría Interna con relación a la seguridad del área de Tecnologías de Información de la Municipalidad de San Carlos, presenta el siguiente informe:

INFORME SOBRE LOS RESULTADOS DE LA AUDITORIA INTERNA RELATIVO A LA SEGURIDAD RAZONABLE DEL ÁREA DE TEGNOLOGÍAS DE INFORMACIÓN EN LA MUNICIPALIDAD DE SAN CARLOS

Artículo I. INTRODUCCIÓN.

Sección 1.01 Origen del estudio.

Este estudio de auditoria se hace en cumplimiento al plan anual de trabajo para el 2009 y de conformidad a las atribuciones conferidas en la Ley General de Control Interno, se llevo a cabo el estudio de fiscalización, análisis y razonabilidad de los Sistemas de Tecnologías de información en la Municipalidad San Carlos.

Sección 1.02 RESPONSABILIDAD DE LA ADMINISTRACIÓN.

La veracidad y exactitud de los datos contenidos en la información suministrada por el Departamento de Tecnologías de información y la Administración, referentes a la seguridad, validez e integridad de las Tecnologías de Información, sobre los cuales se basa el estudio de fiscalización, análisis y razonabilidad, por parte de la auditoría interna, es de total responsabilidad de la administración activa de la Municipalidad de San Carlos.

Sección 1.03 Alcance del estudio.

Para éste estudio se han aplicado técnicas selectivas y de inspección, sin perjuicio de otras observaciones que pueda efectuar esta auditoría interna en cumplimiento de sus funciones de fiscalización.

El estudio se realizó de acuerdo con la normativa jurídica aplicable según las circunstancias, como las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) directrices emitidas por la Contraloría General de la República, según su competencia y las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE). Los datos de la evaluación realizada comprenden del 01 enero 2008 al 30 de octubre del 2009.

Artículo II. RESULTADOS.

Los resultados aquí expuestos están dados en relación al estudio sobre la eficiencia y eficacia de los procesos de control interno realizados por el departamento de Tecnologías de Información de la Municipalidad de San Carlos, en cuanto a razonabilidad, seguridad, validez e integridad de la información que se maneja a través de los sistemas información y los sistemas mismos, con tal propósito se verificó lo siguiente:

2.1 Guía sobre la seguridad del Sistema (SIM).

2.1.1 Privilegio Administrador

En cuanto a este punto, es importante mencionar que la persona o usuario con este privilegio tiene total autonomía (a modificar, eliminar, crear, consultar y/o buscar cualquier información) dentro del sistema (SIM), así mismo, se corroboró mediante una muestra, que existen 16 usuarios y grupos que cuentan con dicho privilegio y de acuerdo al puesto que desempeñan no deberían tenerlo, además no se encontró documentación que indique el por qué estas personas necesitan este privilegio, ejemplo:

En relación a lo anterior, las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) emitida por la Contraloría General de la República, publicada en La Gaceta Nro. 119 del 21 de Junio, 2007 en el punto **1.4.5 Control de acceso,** incisos a, d, e, k donde se indica lo siguiente: La organización debe proteger la información de accesos no autorizados.

Para dicho propósito debe:

a- Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información (…)

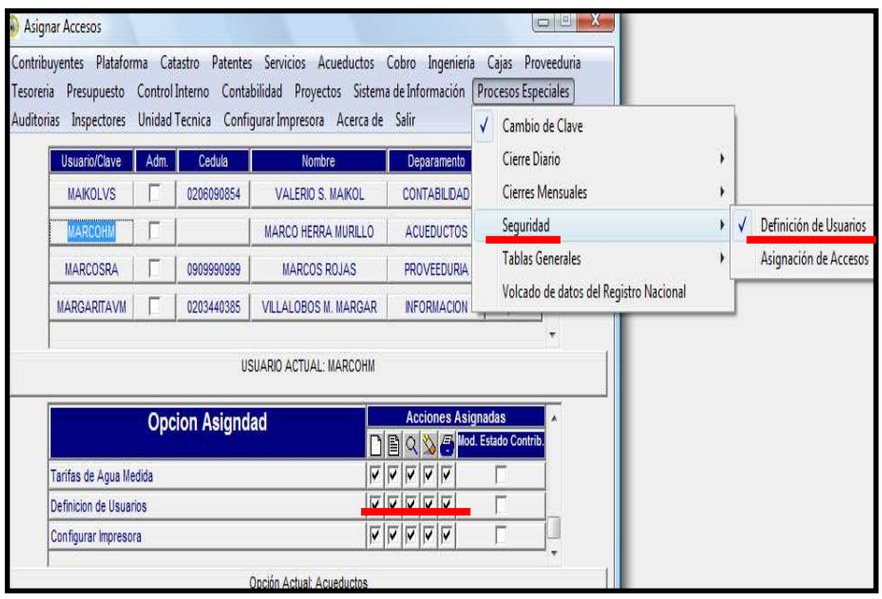
d- Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI.

e- Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de *necesidad de saber o menor privilegio.* (…)

k- Manejar de manera restringida y controlada la información sobre la seguridad de las TI

2.1.2 Definición de usuario y Asignación de accesos

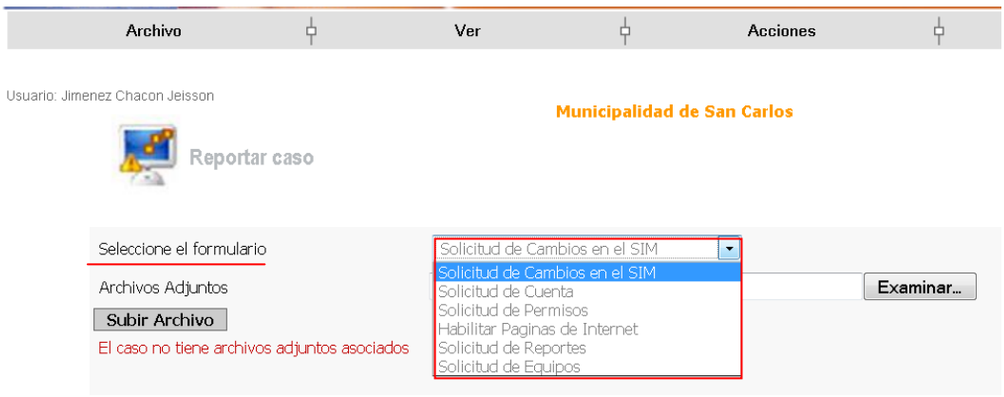
Las Normas de Tecnologías de Información indican en el punto 1.4.5 sobre el Control de los accesos, que la organización debe proteger la información de accesos no autorizados, para ello el Inciso "k" señala que se debe manejar de manera restringida y controlada la información sobre la seguridad de las TI. Ahora bien en el sistema Municipal la *Definición de* usuario y la Asignación de accesos no se encuentran de manera restringida tal y como lo señala la norma, pues como se ve en la siguiente figura que dichos accesos son otorgados a funcionarios que no lo requieren. Esto por cuanto la *Definición de* usuario y Asignación de accesos, son funciones específicas del administrador o encargado del sistema (SIM).



2.1.3 Herramienta ARANDA

De acuerdo a las Normas de Tecnologías de Información en el puntos 4.4 Atención de requerimientos de los usuarios de TI, donde señala que la organización debe hacerle fácil al usuario el proceso para solicitar la atención de los requerimientos que le surjan al utilizar las TI (...) en cuanto a este punto se corroboró que el departamento de TI, si bien elaboró un Manual de Uso del Service Desk (Aranda), esta Auditoría considera que este fue redactado de forma general por cuanto, no explica los diferentes servicios que ofrece TI, tampoco se indica la forma de completar la información de los diferentes formularios, además es

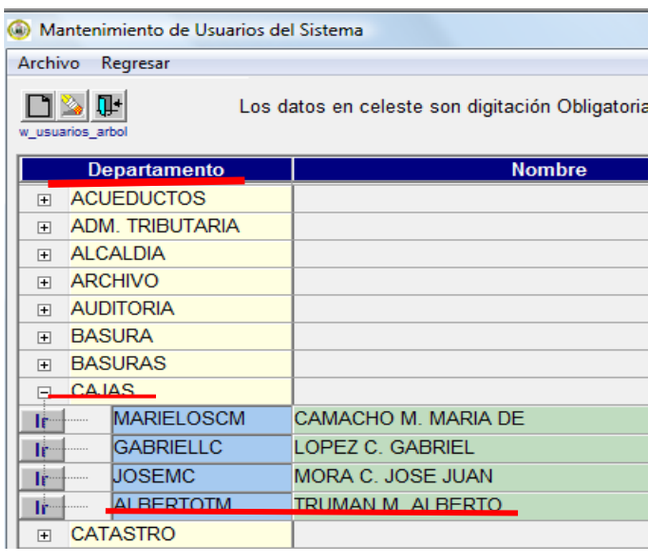
importante mencionar que al 23 de Junio, dentro de la Herramienta ARANDA no existe la opción de desactivar o inactivar un usuario.



2.1.4 Usuarios y departamentos

Se corroboró mediante una muestra obtenida a través del sistema (SIM), que existen 38 usuarios asignados a grupos dentro del Sistema, que no concuerda con el departamento al que pertenece, ni el puesto que desempeña dentro de la Municipalidad de San Carlos, ocasionado con ello que los usuarios tengan accesos y privilegios a módulos dentro del Sistema, no apropiados de acuerdo a sus funciones o puestos que desempeñan, lo que produciría que los datos puedan ser manipulada y la información no sea válida, ni segura. Ejemplo:

Usuario	Nombre de Usuario	Nombre de Grupo SIM	Estado	Grupo actual Municipalidad
ALBERTOTM	TRUMAN M. ALBERTO	CAJAS	ACTIVO	INSPECTORES



Con vista en lo anterior y de acuerdo al punto 1.4.5 Control de acceso de las Normas de Tecnologías de Información, se deberá en especial dar cumplimiento a lo que establecen los incisos “d” y “e” que a la letra dicen:

Inciso d:
“Establecer procedimientos para la definición de perfiles, roles y niveles de privilegios, y para la identificación y autentificación para el acceso a la información, tanto para usuarios como para recursos de TI.”

Inciso “e”:
“Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la Organización bajo el principio de necesidad de saber o menor privilegio.”

2.1.5 Usuarios y Grupos Duplicados.

Se validó mediante una muestra, que existen 4 usuarios y 10 grupos duplicados y activos dentro del Sistema, esto pone en riesgo la integridad y validez de la información que se maneja a través de los sistemas, además es importante mencionar que no se encontró documentación que indique el por qué están duplicados estos usuarios y grupos, esto deja en evidencia un incumplimiento en el punto 1.4.5 control de acceso de las Normas de Tecnologías de Información en el inciso “e” donde señala que se debe asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio. (…) Ejemplo:

Grupos Duplicados

Usuarios Duplicados

2.1.6 Ex – funcionarios que se encuentran activos en el sistema

Se corroboró mediante una muestra obtenida a través del sistema (SIM) que existen 10 usuarios Activos, referentes a personas que ya no laborar para la institución, es importante mencionar que la existencia de usuarios activos asociados a ex-funcionarios incrementa el riesgo de que se efectúen transacciones no autorizadas sobre la información sensible de la Municipalidad de San Carlos, situación que podría comprometer la validez y confidencialidad de la información. Ejemplo:

En base a lo anterior y de acuerdo a las Normas de Tecnologías de Información en los puntos 1.4.5 Control de acceso, incisos (f, k) donde se indica que la organización debe proteger la información de accesos no autorizados y para dicho propósito debe:

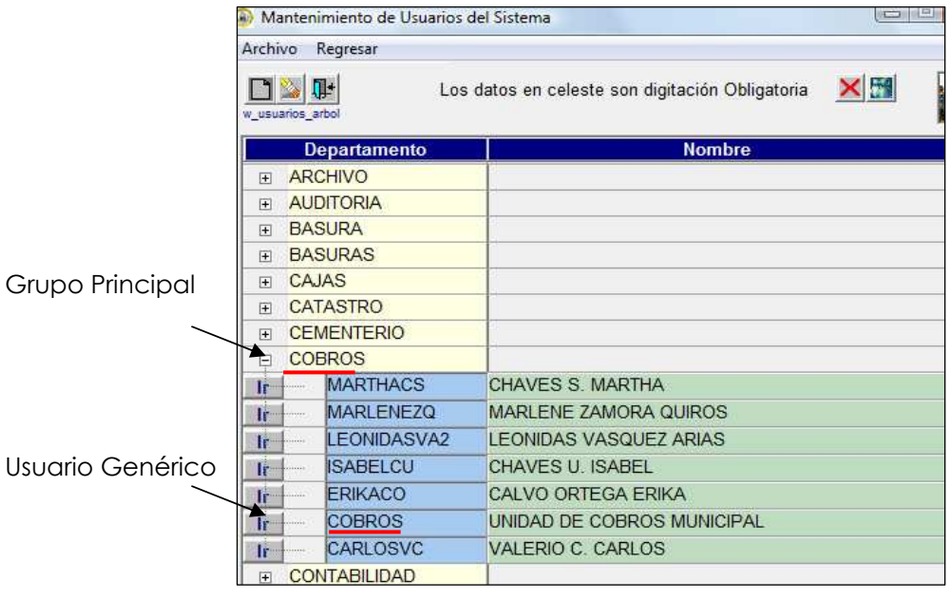
> Inciso f:
> "Implementar el uso y control de medios de autenticación (identificación de usuarios, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autentificación, así como para su revisión y actualización periódica y atención de usos irregulares."
>
> El inciso "k":
> "Manejar de manera restringida y controlada la información sobre la seguridad de las TI."

2.1.7 Usuarios y grupos Genéricos

Se corroboró mediante una muestra, que existen 36 Usuarios y Grupos genéricos dentro de los Grupos Principales del sistema, esto incrementa el riesgo de que se efectúen transacciones no autorizadas sobre la información sensible de la Organización, es importante mencionar que no se encontró documentación que indique la persona responsable de estos usuarios y grupos, situación que podría comprometer la validez y confidencialidad de la información.

En relación a lo anterior y de acuerdo a las Normas de Tecnologías de Información, donde indica que la organización debe proteger la información de accesos no autorizados y para dicho propósito se debe señalar el punto 1.4.5 Control de acceso en él Inciso "k" que a la letra dice: "Manejar de manera restringida y controlada la información sobre la

seguridad de las TI.", a la vez es importante mencionar el punto 4.3 Administración de datos donde se menciona que "la organización debe asegurarse de que los datos que son procesados mediante TI corresponden a transacciones validas y debidamente autorizadas. (…)" Ejemplo:



2.1.8 Ciclo de vida del Sistema

De acuerdo a las Normas de Tecnologías de Información en el puntos 3.2 Implementación de software, incisos "b", donde se indica que la organización debe desarrollar y aplicar un marco metodológico que guíe los procesos de implementación y considere la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación post-implementación de la satisfacción de los requerimientos.

De acuerdo a lo anterior, es importante mencionar que no se encontró documentación que evidencie los pasos o procesos que se realizaron para el desarrollo del sistema, como lo son:

- *La documentación del sistema*: que tiene como finalidad, dar a conocer, describir y comprender lo que hace el sistema, su ambiente, sus limitaciones y los controles incorporados, proporcionando a todos los interesados una compresión clara y confiable del sistema, esta documentación es conocida como Manual del Sistema.

- *La documentación del programa*: también conocida como Manual de programas, por lo general incluye el código y título o nombre del programa(s), la descripción del programa en forma narrativa, el diagrama de lógica o algoritmo y tabla de decisiones si las hubieran, formato y descripción de los archivos, listado de los controles, instrucciones de operación, registro de cambios a los programas y su autorización, listado de la última corrida de pruebas y demás información pertinente.

- La *documentación del usuario:* Esta por lo general, incluye de forma detallada y organizada los servicios que brinda el sistema de manera

que los usuarios sean autosuficientes en el manejo del sistema, importante mencionar que debe presentarse en un lenguaje corriente, evitando la jera computacional.

2.1.9 Perfiles para los usuarios del SIM.

En la evaluación de este punto es importante mencionar que el sistema SIM no cuenta con un proceso para la definición de perfiles y de acuerdo a las Normas de Tecnologías de Información en el punto 1.4.5 sobre el Control de los accesos, donde indica que la organización debe proteger la información de accesos no autorizados y para ello señala el inciso (d) que a la letra dice “Establecer procedimientos para la definición de perfiles, roles y nivel de privilegio, y para la identificación y autentificación para el acceso a la información, tanto para usuarios como para recursos de TI.”

2.1.10 Accesos y privilegios para los usuarios del SIM.

Se validó mediante entrevistas y solicitudes registradas en la herramienta ARANDA que los jefes requieren de mayor capacitación y documentación que les permita realizar las solicitudes a TI de accesos y privilegios para un usuario en el Sistema SIM, esto por cuanto las Normas de Tecnologías de Información en los puntos 1.4.2 Compromiso del personal con la seguridad de la información, donde indica que el personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riegos de error humano, robo, fraude o uso inadecuado de los recursos de TI, y para ello señala el inciso (a) que a la letra dice “Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.

2.1.11 Pase a producción en el Sistema SIM

No se encontró documentación sobre los procesos que se realizar a la hora de hacer un pase a producción ni sobre las supervisiones ejecutadas por el jefe al momento de ejecutar este proceso**,** en cuanto a este punto las Normas de Tecnologías de Información señalan:

- 1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica, indica que la organización debe mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o perdida de información y para este propósito señala el inciso (b) “Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura.”.

- 3.2 Implementación de software, inciso (d) que a la letra dice “Controlar la implementación del software en el ambiente de producción y garantizar la integridad de datos y programas en los procesos de conversión y migración.”

- 4.2 Administración y operación de la plataforma tecnología, inciso (e) “Controlar la ejecución de los trabajos mediante su programación, supervisión y registro”

2.1.12 Registro de las fallas o errores

De acuerdo a las Normas de Tecnologías de Información en el punto 4.2 Administración y operación de la plataforma tecnología, donde indica que la organización debe mantener la plataforma tecnológica en optimas condiciones y minimizar su riesgos de fallas, para ello señala el inciso (b), que a la letra dice "vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas" , cabe resaltar el punto 4.5 Manejo de incidentes, que expresa que la organización debe identificar, analizar y resolver de manera oportuna los problemas, errores e incidente significativos que se susciten con las TI. Además, debe darles el seguimiento pertinente, minimizar el riesgo de recurrencia y procurar el aprendizaje necesario

Con vista en lo anterior, es importante mencionar que no se encontró documentación sobre las fallas o errores presentados en el Sistema SIM (Sistema Integrado Municipal).

2.2 Guía de Bases de Datos SQL Server 2005

2.2.1 Políticas de contraseña y de Expiración de contraseñas

Se corroboró que en la Base de Datos SQL Server 2005, existen usuarios que no tienen activas las políticas de contraseña y/o la de Expiración de contraseñas, en cuanto a este punto las Normas de Tecnologías de Información señalan 1.4.5 Control de acceso, la organización debe proteger la información de accesos no autorizados y para dicho propósito el incisos (a) indica, "Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación". Ejemplo:

Usuario Login de la Base de Datos SQL Server 2005

2.2.2 Usuarios dentro de la Base de Datos

No se encontró documentación sobre los procesos que se realizar a la hora de crear y eliminar(o desactivar) un usuario dentro de la Bases de Datos SQL Server 2005, en cuanto a este punto las Normas de Tecnologías de Información señala 1.4.5 Control de acceso, la organización debe proteger la información de accesos no autorizados para dicho propósito el inciso (a) expresa "Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al

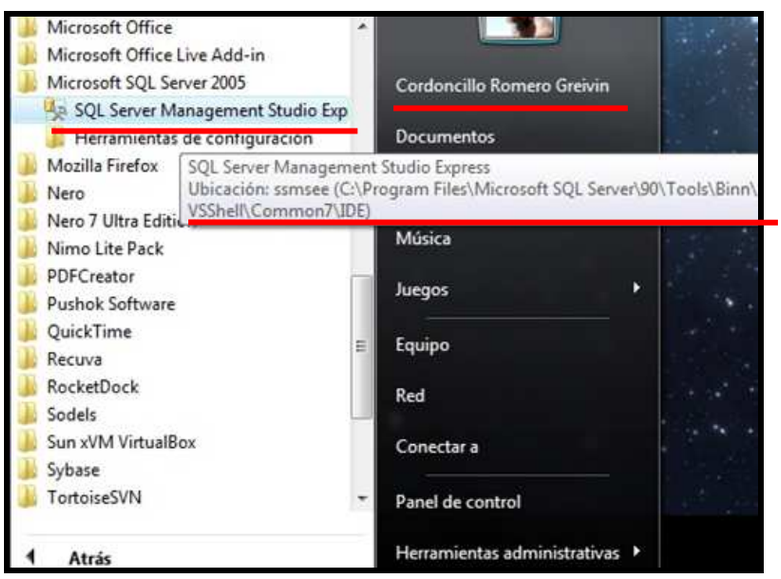
software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación.

2.2.3 Accesos de la base de datos

Se verificó que todo el departamento de TI, incluyendo área de desarrolladores (programadores) y telecomunicaciones tiene ***acceso directo*** a la Base de Datos SQL Server 2005, la persona que ingresa por medio de este acceso tiene los privilegios para modificar, eliminar, crear, consultar y/o buscar cualquier información dentro de la base de datos, sin embargo se corroboró que no existen usuarios que detallen de forma individual al personal del departamento de TI, por otra parte es importante mencionar que no se encontró documentación sobre las políticas, reglas o procedimientos relacionados con el acceso a la Bases de Datos ni al software de Bases de Datos, en cuanto a este punto las Normas de Tecnologías de Información señalan 1.4.5 Control de acceso, donde se destaca los incisos (a- e) que a la letra dicen:

> Inciso “a”:
> Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación.
>
> Inciso “e”:
> Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la Organización bajo el principio de necesidad de saber o menor privilegio.

A la vez es importante mencionar el punto 1.4.1 Implementación de un marco de seguridad de la información, inciso (c) en el cual la organización debe documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados. Ejemplo:



2.2.4 Función a nivel de Servidor (sysadmin).

Se corroboró que existen usuarios que no requieren la función de sysadmin, esta función permite realizar cualquier actividad en el servidor de Base de Datos (como los es, agregar inicios de sesión de SQL Server, cuentas de Windows y grupos de Windows).

En base a lo anterior y de acuerdo las Normas de Tecnologías de Información en el punto 1.4.5 Control de acceso, donde expresa que la organización debe proteger la información de accesos no autorizados y para dicho propósito el inciso (d) indica, “Establecer procedimientos para la definición de perfiles, roles y nivel de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI.

2.2.5 Función a nivel de base de datos (db_owner)

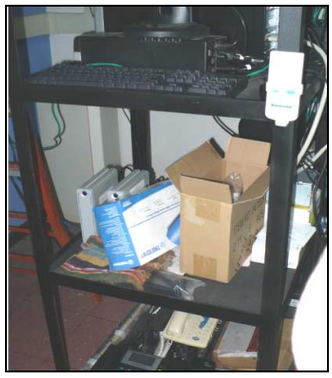
Se corroboró que existen usuarios que no requieren la función db_owner la cual es utilizada para realizar todas las actividades de configuración y mantenimiento en la base de datos.

Con fundamento en lo anterior, las Normas de Tecnologías de Información en el punto 1.4.5 Control de acceso, donde expresa que la organización debe proteger la información de accesos no autorizados y para dicho propósito el inciso (d) indica, “Establecer procedimientos para la definición de perfiles, roles y nivel de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI.

2.3 Guía de Seguridad Física y Ambiental

2.3.1 Cuarto de servidores

La Normas Técnicas para la Gestión y el Control de las Tecnologías de Información en el punto 1.4.3 Seguridad física y ambiental, señala que se deben proteger los recursos de TI estableciendo ambientes físicos seguros y controlados, sin embargo se observó que dentro del cuarto de servidores existen cajas y equipos sin uso, no aptos o adecuados para estar dentro de este aposento.



2.3.2 Mantenimiento de servidores

En cuanto al mantenimiento de los servidores, se indicó por funcionarios de TI, que este lo realizan ellos, sin embargo no hay certeza de cada cuanto tiempo se hace el mantenimiento sobre los servidores, pues no existe un registro documental que permita verificar o corroborar dicho proceso, es importante indicar que las Normas de Tecnologías de Información en el punto 1.4.3 sobre Seguridad física y ambiental señalan que se debe proteger los recursos de TI estableciendo ambientes físicos seguros y controlados, para dicho propósito el inciso (d) expresa que la organización debe controla los servicios de mantenimiento.

2.3.3 Extintores y su debido mantenimiento.

En relación a este punto la Norma 1.4.3 Seguridad física y ambiental, se indica en el inciso “h” que como parte de la protección se deben considerar los riegos asociados con el ambiente, y como se observa en las fotos siguientes en el departamento de TI cuenta con un extintor que podría ser de gran ayuda ante una eventualidad o riesgo, es de suma importancia que el extintor reciba un eficaz control de mantenimiento, ya que se puedo comprobar que el último mantenimiento recibido fue en setiembre del 2006.

2.3.4 Detectores de Humo

La Normas de Tecnologías de Información en el punto 1.4.3 Seguridad física y ambiental, señala que se deben proteger los recursos de TI estableciendo ambientes físicos seguros y controlados, sin embargo se corroboró que se no cuenta con la existencia detectores de Humo en el departamento de TI y mucho menos en el resto de la Institución, lo que representa un riegos asociados con el ambiente, que a la fecha no ha sido atendido en forma oportuna

2.3.5 Bitácoras de acceso

Se verificó que no se cuenta con bitácoras de acceso al cuarto de servidores ni del departamento de TI, de acuerdo a las Normas de Tecnologías de Información, el punto 1.4.3 Seguridad física y ambiental,

indica que la organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, para dicho propósito se señalan los incisos (a-g).

2.3.6 Riesgos Ambientales

Se identificó que existe un riesgo ambiental latente que podría afectar la seguridad del cuarto de servidores y al departamento de TI, por cuanto los servicios sanitarios de hombres, están ubicados a un costado del departamento de TI, el cual es un riesgo ambiental que podría afectar la seguridad de los equipos y la información de ocurrir derrames de aguas negras o pluviales, en cuanto a este punto se debe contar con las medidas de control pertinentes para minimizar dicho riesgo tal y como lo señala la Norma 1.4.3 en el inciso “h”.

2.4 Guía de Respaldos

2.4.1 Proceso de respaldos

Se verificó que, los respaldos de la Bases de Datos SQL Server 2005 son almacenados de forma local en el servidor de Bases de Datos, además es importante mencionar que los respaldos físicos (respaldos externos al servidor de Bases de Datos) son realizados cada tres días o cuando lo amerite, ósea en caso de un imprevisto o falla.

Con vista en lo anterior, las Normas de Tecnologías de Información en el punto 4.2 Administración y operación de la plataforma tecnológica inciso (h), señala que se debe “Definir formalmente y efectuar rutinas de respaldos, custodiar los medios de respaldos en ambientes adecuados, controlar el acceso a dichos medios y establecer procedimientos de control para los procesos de restauración.”

2.4.2 Almacén de respaldos

Se observó que los respaldos de la Base de Datos se encuentran en el departamento de TI, importante mencionar que estos, son almacenados en estantes al alcance de todas las personas que ingresen al departamento, además mencionar que no existen contratos con entidad externa, para el resguardo de dichos respaldos.

De acuerdo a las Normas 1.4.4 Seguridad en las operaciones y comunicaciones, inciso (b) donde señala que se deben “Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativo al manejo y desecho de esos medios”, además el punto 1.4.5 Control de acceso inciso (i) expresa que se debe establecer controles de acceso a la información almacenada en medios físicos y proteger adecuadamente dichos medios. Ejemplo:

Artículo III. CONCLUSIONES:

Luego de lo investigado y analizado, esta auditoría concluye que la Administración Municipal y sobre todo el departamento de TI, deberán dar cumplimiento a Ley General de Control Interno –Ley 8292, y a las Normas Técnicas para la Gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) en especial a los criterios básicos de control que deben observarse en la gestión de esas tecnologías y que tiene como propósito coadyuvar en su trabajo, en virtud de que dicha tecnología se ha convertido en un instrumento esencial en la prestación de los servicios públicos, representando inversiones importantes en el presupuesto de la Municipalidad de San Carlos.

De conformidad con la evaluación realizada, el control interno no proporciona una seguridad razonable, por cuanto se presentan irregularidades en la Gestión documental, en la calidad de la información en lo que respecta a confiabilidad, en la falta de controles eficientes para los sistemas de información, sin embargo es importante mencionar que los controles internos son una herramienta útil para la Administración activa y en especial para el departamento de TI.

Congruente con el ordenamiento jurídico, es responsabilidad del jerarca y del titular subordinado establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional en aras del cumplimiento de los objetivos institucionales y del uso adecuado de los recursos públicos empleados para ello.

Artículo IV. RECOMENDACIONES.

Sección 4.01 AL CONCEJO MUNICIPAL.

(a) CON EL FIN DE DAR CUMPLIMIENTO A LO INDICADO EN LA LEY GENERAL DE CONTROL INTERNO Nº 8292 Y LAS NORMAS TÉCNICAS PARA LA GESTIÓN Y EL CONTROL DE LAS TECNOLOGÍAS DE INFORMACIÓN (N-2-2007-CO-DFOE) Y LA DEMÁS NORMATIVA LEGAL VIGENTE, TOMAR LAS ACCIONES PRECISAS CON EL FIN DE IMPLEMENTAR LOS SISTEMAS DE CONTROL INTERNO A EFECTO DE FACILITAR LA CONSECUCIÓN DE LOS OBJETIVOS, AJUSTÁNDOSE A LOS CRITERIOS DE LEGALIDAD, TRANSPARENCIA Y EFICIENCIA; Y FIJAR UN CRONOGRAMA DE PLAZOS A LA ADMINISTRACIÓN DE LAS ACTIVIDADES ACORDADAS PARA EL CUMPLIMIENTO A LAS RECOMENDACIONES SEÑALADAS EN EL PUNTO 4.2.

(b) COMUNICAR A ESTA AUDITORÍA DE CONFORMIDAD AL ARTÍCULO 37 DE LA LEY GENERAL DE CONTROL INTERNO 8292 EN LOS PRÓXIMOS 30 DÍAS HÁBILES, CONTADOS A PARTIR DE LA FECHA DE RECIBO DE ESTE INFORME, LOS ACUERDOS TOMADOS EN RELACIÓN CON LAS RECOMENDACIONES CONTENIDAS EN ESTE INFORME.

Sección 4.02 A LA ALCALDÍA MUNICIPAL.

(a) QUE DE CONFORMIDAD A LAS NORMAS DE CONTROL INTERNO PARA EL SECTOR PÚBLICO (N-2-2009-CO-DFOE), SEGÚN SUS COMPETENCIAS GIRE INSTRUCCIONES PRECISAS A SUS TITULARES SUBORDINADOS PARA QUE SE DISEÑE E IMPLEMENTE UN SISTEMA DE CONTROL INTERNO A FIN DE ASEGURAR RAZONABLEMENTE LOS SISTEMAS DE INFORMACIÓN, TOMANDO EN CUENTA EL BLOQUE DE LEGALIDAD Y LOS RIESGOS RELEVANTES

(b) GIRAR INSTRUCCIONES CLARAS AL COORDINADOR DE TI, PARA QUE DE CUMPLIMIENTO A LAS NORMAS TÉCNICAS PARA LA GESTIÓN Y CONTROL DE LAS TECNOLOGÍAS DE INFORMACIÓN EN RELACIÓN A:

1. Depurar los usuarios con el privilegio Administrador, eliminando este privilegio a los usuarios que no lo requieran, según el punto (2.1.1)

2. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, además, quitarle a los usuarios los accesos que de acuerdo a sus funciones o puestos no debería tenerlos. ver el punto (2.1.2)

3. Mejorar el manual de Uso del Service Desk, especificando los servicios, indicando la manera de completar la información, facilitando al usuario el uso de esta herramienta, a la vez implementar dentro de la Herramienta ARANDA la opción de desactivar o inactivar un usuario, punto (2.1.3)

4. Depurar los usuarios, grupos y departamentos en el sistema SIM, eliminando duplicaciones, ordenando los usuarios de acuerdo a su departamento o puesto que desempeñan dentro de la organización, dejando activos solo los usuarios que están laborando, y además documentar los usuarios genéricos, eliminando los que no se requieran. Según los puntos (2.1.4, 2.1.5, 2.1.6, 2.1.7).

5. Documentar todos los procesos que realiza el departamento de TI, y en especial los procesos que se realizan a la hora de desarrollar un sistema, los pases a producción, las supervisiones de estos procesos, registro de fallas o errores que da el sistema, y la creación o eliminación (desactivación) de los usuarios de la Base de Datos . Puntos (2.1.8, 2.1.11, 2.1.12, 2.2.2)

6. Establecer políticas, reglas y procedimientos para la definición de perfiles de usuarios dentro del sistema, según los puntos (2.1.9)

7. Promover la capacitación que le facilite a los encargados realizar solicitudes sobre los accesos y privilegios que requiera un usuario. Punto 2.1.10

8. Activar las políticas de contraseña y expiración de contraseña sobre los usuarios de la Bases de Datos SQL Server 2005. Ver punto 2.2.1

9. Eliminar el acceso directo a la Base de Datos a aquellas personas que no tengan la función específica de un DBA (Data Base Administrator). Ver Punto (2.2.3)

10. Eliminar de los usuarios las funciones que no requieren a nivel de Servidor (Sysadmin) y a nivel de Base de Datos (db_owner), ver puntos (2.2.4, 2.2.5)

11. Extraer del cuarto de servidores equipo y material no aptos para estar en dicho aposento. Ver 2.3.1

12. Elaborar o llevar un registro del mantenimiento que reciben los servidores. Ver (2.3.2)

13. Dar mantenimiento adecuado a los extintores e implementar detectores de humo dentro de la Organización. Ver (2.3.3, 2.3.4)

14. Implementar bitácoras de acceso al cuarto de servidores y al Departamento de TI. Ver punto(2.3.5)

15. Implementar medidas de seguridad para evitar que desperfectos en el servicio sanitario contiguo al Departamento de TI dañe los equipos electrónicos. Ver punto(2.3.6)

16. Realizar rutinas de respaldos físicos (respaldos externos al servidor de Bases de Datos) de forma diaria, semanal, y mensual, que permitan resguardar toda la información de la Base de Datos e implementar los procesos de restauración de los mismos. Ver punto (2.4.1)

17. Definir un lugar seguro para el almacenamiento de los respaldos físicos, tomando en cuenta la opción de que estos sean almacenados en una entidad externa. Ver Punto (2.4.2)

(c) COMUNICAR A ESTA AUDITORÍA INTERNA DE CONFORMIDAD AL ARTÍCULO 36 DE LA LEY GENERAL DE CONTROL INTERNO Nº 8292, EN LOS PRÓXIMOS 10 DÍAS HÁBILES CONTADOS A PARTIR DE LA FECHA DE RECIBO DE ESTE INFORME, LAS ACCIONES Y CRONOGRAMA DE PLAZOS PARA LA IMPLEMENTACIÓN DE LAS ACTIVIDADES QUE SE LLEVARÁN A CABO PARA EL CUMPLIMIENTO DE LAS RECOMENDACIONES CONTENIDAS EN ESTE DOCUMENTO.

El Regidor Suplente, Carlos Corella Chaves consulta si se tiene a una persona responsable para que se encargue de que las recomendaciones se cumplan, y que se le aclaren algunos puntos del informe.

El Licenciado Fernando Chaves Peralta, Auditor interno de la Municipalidad de San Carlos explica que este informe fue presentado primeramente a la Administración para su análisis, este informe lo que lleva a mejorara muchas deficiencias que creemos de acuerdo a la normativa que ya tenían que estar casi implementados muchos manuales por que se le había dado seis meses para que la Municipalidad de San Carlos tuviera grafico de lo que había echo. Desde hace diez años hay un Manual de Control Interno que ya había establecido como se debe manejar el departamento de Tecnologías de Información, es la Administración y no la Auditoría la que debe estar revisando, evaluando esos riesgo par que no vayan a suceder.

La Ingeniera Tracy Delgado Zamora explica que en el punto 2.1.7., en el cual se consulta quien es el usuario cobros, coros actualmente no corresponde a ningún funcionario, es un usuario genérico y no se encontró documentación que identifique a quien corresponde este usuario o a quien pertenece. Es por esto que se hace la observación que si se necesita ese usuario que lo identifique q quien corresponde o para qué sirve este usuario por que tiene acceso a diferentes módulos. En el punto 2.1.5. Usuarios y Grupos Duplicados se ve como la compañera Bernardita tiene dos usuarios y existen aproximadamente cuatro grupos duplicados y diez usuarios, esto significa que una persona que tiene dos usuarios puede hacer cosas con los dos usuarios, entonces a cual de los dos usuarios responsabiliza usted de efectuar

transacción si los dos corresponden a la misma persona. Este informe es referente a observaciones que el departamento debe mejorar y se les da un tipo de guía para que lo realicen. En las conclusiones con respecto al punto 17, quiere decir que es importante que se contrate o se tenga alguna entidad externa que tenga el resguardo de los respaldos, por que es información muy sensible que día con día estamos llegando en los sistemas, no estoy diciendo que están inseguros en la Municipalidad de San Carlos, si no que esto es una medida preventiva en caso que ocurra alguna eventualidad en la Municipalidad, podemos tomar la información de otro lugar.

El Regidor Ricardo Rodríguez, menciona que los extintores pueden provocar un gran problema ya que tienen fecha de setiembre del 2006, se tiene equipo alquilado el cual están bajo una póliza, si mañana ocurre sucede un incendio, el instituto buscaría la manera de quitarse de esa póliza por cuanto los extintores están vencidos.

La Regidora Ada Luz Chavarría se refiere al caso de los usuarios genérico, en caso que se hubiera dado alguna modificación, alteración o cualquier situación en este sistema a quien se responsabilizaría si eventualmente se desconoce quien es. Esto es de gran preocupación por que con este informe se analiza que es lo que se ha estado haciendo y hasta donde se ha estado velando por el verdadero buen funcionamiento de los departamentos, y lo importante que es que esta auditoría sea realice por departamentos. Es momento de pensar en todo lo que hay que mejorar, esta es una empresa grande en la que se debe velar por el buen funcionamiento.

La Regidora Marcela Céspedes Rojas, menciona que es alarmante escuchar todo esto. Es bueno este tipo de informe por que permiten detectar cuales son esas debilidades que hay en los departamentos para poder mejorarlo. Las recomendaciones son muy atinadas, y se deberían cumplir y que se informe al Concejo los avances que se van dando en el departamento de informática y que no solo se informe a la Auditoría.

El Ingeniero Maikel Quirós González, del Departamento de TI, de la Municipalidad de San Carlos, manifiesta que el informe que están presentado ante el Concejo no es el mismo que les presentaron a ellos anteriormente, por lo que se sentará a leerlo y traer respuesta a todo esto. Además señala en la Ingeniera Tracy Delgado en Algún momento solicito ayuda a terceros divulgando información que es confidencial, para la realización del informe que está presentado.

El Presidente Municipal, Gerardo Salas Lizano señala que no se tomará ningún acuerda ya que en el informe se están dando treinta días hábiles para que el Departamento de TI responda a este informe. Y dar la oportunidad ha este departamento para que nos venga a explicar punto por punto todo lo mencionado.

La Regidora Marcela Céspedes Rojas, indica que le gustaría escuchar tanto el punto de vista de cada uno de los puntos por parte del Departamento de Informática como lo que tiene que decir el Departamento de Auditoría con relación a lo señalado por el Ingeniero Maikel Quirós, esperando que esto sea lo más pronto posible.

El Regidor Suplente Carlos Corella, señala que no sería bueno que se contrate a gente profesional o empresas privadas para que realicen este estudio, esto sería un paso hacia atrás. Hay que tener claro que la Auditoría es el que nos da el paso a seguir si un acuerdo está bien tomado o alguna contratación a una empresa.

El Licenciado Fernando Chaves aclara que hay una normativa, la Ley de Control Interno, hay un periodo para apelación. Este trabajo está sustentado, hay evidencia y se debe leer muy bien las cosas para no hacer malas interpretaciones. Con respecto a los extinguidores ahí los tiene pero no los están revisando. Por otra parte si tienen problemas de recursos humanos eso es otro problema pero no hay que dejar otras

cosas abiertas. Y el área de las consultorio o no consultorías, el Ingeniero Quirós menciona que la información se les pasó a terceros y eso hay que demostrarlo, por que una cosa es consultar el tipo de normativa y como se administra una base de datos a dar una base de datos. Lo más importante en todo esto es que se mejoren muchas cosas.

La Ingeniera Tracy Delgado Zamora, menciona que ella en ningún momento divulgo información de la Municipalidad, que solicito ayuda de colegas de trabajos anteriores, para hacer las guías con las que se realizó este informe, por que son guías que no solo una persona puede realizar, son todas las personas juntas, además señala que estos seis meses no ha pasado con los brazos cruzados, por que no hizo solo esta guía se hicieron todas las guías. Por otra parte cuando se refiera a los usuarios duplicados que si se tiene por estrategia, dónde se encuentra la documentación, la observación salió precisamente por que no hay documentación al respecto. Además cuando se le pedía información al Ingeniero Quirós no la brindaba inmediatamente si no mucho tiempo después lo que retraso en cierto modo la realización de este informe. Igualmente señala que si este informe está como está es por que tiene pruebas suficientes y pertinentes para decir lo que se dice.

El Presidente Municipal, Gerardo Salas Lizano, señala que para la sesión del lunes 11 de enero del 2010, se presente el punto de vista del Departamento de TI, y que los compañeros de Auditoría también estén presentes en esa sesión.

AL SER LAS 15:28 HORAS, EL SEÑOR PRESIDENTE MUNICIPAL, DA POR CONCLUIDA LA SESIÓN.--

Gerardo Salas Lizano
PRESIDENTE MUNICIPAL

Alejandra Bustamante Segura
SECRETARIA DEL CONCEJO MUNICIPAL

ABS