AUDITORÍA SISTEMAS INFORMÁTICOS

MUNICIPALIDAD SAN PEDRO DE ATACAMA

INTRODUCCION

En cumplimiento del plan anual de auditorías y las facultades que el artículo 29 de le Ley N° 18.695, Orgánica Constitucional de Municipalidades, le entrega a la Dirección de Control, para efectuar Auditorías Operativas, se ha establecido los fines y objetivos a llevar en esta auditoría.

OBJETIVO:

El objetivo de la auditoría consiste en revisar y evaluar aspectos relacionados con Políticas, Normas, Prácticas y Procedimientos relacionados con tecnologías de la información y comunicaciones (TIC), incluidas aquellas actividades que se hacen de manera manual o no automatizada, que se desarrollan en torno a los sistemas.

METODOLOGIA:

El Trabajo se efectuó en conformidad a las normas y procedimientos de control aceptados por la Contraloría General de la República e incluirá pruebas de validación respectivas, sin perjuicio de utilizar otros medios técnicos estimados necesarios para circunstancias determinadas.-

ALCANCES:

La Auditoría comprenderá a las Unidades Municipales y los Servicios Traspasados de Salud y DAEM, en los siguientes ITEM´s

- Controles Generales de las Tecnologías de la Información.-
- Controles de Seguridad Física

- 100 del Ministerio Secretaría General de la Presidencia, que aprueba las normas técnicas para el desarrollo de los sitios WEB de los órganos de la Administración Pública.- Todos del Ministerio Secretaría General de la Presidencia.-

En la auditoría se examinarán los temas relacionados con tecnología de información en régimen operativo y que tengan directa relación con transacciones automatizadas de los sistemas operativos administrativos municipales.

Se efectuará un análisis de los procedimientos municipales específicos y la aplicación de controles, con la finalidad de verificar que la seguridad implantada en los procesos brinde a las transacciones de los sistemas el resguardo operacional adecuado.-

Se informará en los siguientes ámbitos

1.- Procesos Significativos Asociados a TI.-

2.- Estructura Organizacional de la Unidad de Informática

3.- Diagrama de Red

4.- Proyectos Vigentes

a. Sistemas

b. Infraestructura Tecnológica

- **Redes**
- **Redes Inalámbricas**
- **Enlace de Datos y Telefonía**
- **Seguridad**
  - **Servidores**

5.- Aspectos de Control Interno Sobre Procesos TI y El Riesgo de Fraude

a. **Control Interno:**

sistemas administrativos por parte de personas no autorizadas, grabación, emisión, impresión y de otros procesos informativos que involucren datos sensibles.-

2. **Inventario de Equipamiento Informático:** Se debe verificar la existencia de un inventario de equipamiento informáticos, tecnológicos y de comunicación.-
3. **Registro de Equipamiento Informático:**
    a. Verificar que exista un control de movimiento de equipos informáticos y si estos se han entregado mediante un acta de entrega y recepción de los equipos.
    b. Verificar la existencia de una política de seguridad y control de equipos utilizados en terreno.-
4. **Licencias:**
    a. Verificar que el municipio cumpla con el licenciamiento de las plataformas de software de operaciones.-
5. **Seguridad Física:**
    a. Se debe verificar que la seguridad física de la sala de servidores cumpla con los siguientes atributos.
        1. **Circuitos Eléctricos Certificados.**
        2. Que los muros y techumbre cumplan con los requisitos mínimos en aspectos como sismicidad, control de incendios, control de polvo, control de temperatura, humedad, etc.
        3. Circuito cerrado de televisión, alarmas de seguridad de ingreso, sensores de humo, humedad y temperatura.
        4. Iluminación artificial suficiente para trabajos al interior.
        5. Canalización adecuada de cables eléctricos y de redes.
        6. Bitácora de mantenciones realizadas.-

        - Boletas de Garantía
    - Sistemas de Patentes Comerciales
    - Sistema de Permisos de Circulación

b.- Tipos de Usuarios: Verificar que las distintas cuentas de usuarios estén asignadas y sean utilizadas para interactuar con todos los sistemas, por perfiles y atributos. Verificar la adecuada entrega de atributos por usuario, que el mantenedor opere por nombre y clave habilitada para cada tipo de acceso.

c.- Evaluación de la Integridad de la Información: ¿La Municipalidad de San Pedro de Atacama, cuenta con bases de datos, donde se alojen tablas de registros , que tengan directa relación con los procesos significativos asociados a TI y que administran datos críticos. En el caso de control de acceso lógico, se evaluará la cantidad de personal activo, pasivo y su relación contractual con el municipio, validando la integridad de datos relevantes, con el fin de comparar la información procesada con las cuentas de usuarios activos para un funcionario y los permisos otorgados para dicha cuenta.

d.- Control de Datos Numéricos: Verificar la presencia de fallas en los controles de validación existentes en cualquier campo (Vgr., En permisos de circulación número de motor).-

e.- Control de Validación en Ingreso de Datos: Verificar la existencia de control de validación del ingreso de datos erróneos.

f.- Verificación del Modelo de Datos. Se verificará la existencia de documentación relativa al diseño lógico de la base de datos que soporta los sistemas municipales implantados por distintas empresas (Vgr., CAS CHILE).-

12.- Cumplimiento de Decretos: Se deberá verificar el cumplimiento de los siguientes Decretos Supremos:

a.- D.S. 77 de 2004 del Ministerio Secretaría General de la Presidencia, que regula de manera general y supletoria las comunicaciones entre órganos del Estado y las de estos con personas de aquellos ámbitos no regulados por esta norma, particularmente en los siguientes aspectos:

1. El Municipio, ¿Declara en el o en los sitios WEB de su institución, cuales son los formatos utilizados para el envío, autenticación y acceso a información disponible?.-
2. ¿La Municipalidad almacena las comunicaciones electrónicas mantenidas con usuarios/beneficiarios, por lo menos durante 6 años en el repositorio?.
3. ¿La Municipalidad adjunta los antecedentes para permitir la búsqueda y recuperación de la documentación almacenada en los repositorios de documentos electrónicos?.-
4. En el caso que se verifique una comunicación electrónica a una dirección de correo que no admita ser calificada como apta, al tenor de lo señalado en el artículo 3, letra d) de los Decretos Supremos ya referidos precedentemente; ¿Existe, por parte del municipio, una normativa que regule el procedimiento de respuesta al recurrente y remisión de los antecedentes a la autoridad competente?

b.- D.S. 81 y 83, ambos de 2004, del Ministerio Secretaría General de la Presidencia, sobre Documentos electrónicos, firma digital y firma digital avanzada.

c.- Decreto Supremo N° 93 del año 2006, del Ministerio Secretaría General de la Presidencia, que aprueba normas técnicas para la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes masivos, no

1. ¿El municipio contempla en el desarrollo de sus sitios WEB, rangos de disponibilidad y accesibilidad de la información y/o el resguardo de los titulares de los derechos?
2. ¿El Municipio desarrolla tareas que permitan implementar en sus sitios WEB, las directrices principales de las normas internacionales sobre accesibilidad para personas discapacitadas?
3. ¿La unidad de informática realiza un monitoreo acerca del cumplimiento de los procedimientos establecidos, de manera de reducir los costos asociados a la recepción de Mensajes Masivos no Deseados y que no guarden relación con los asuntos propiamente municipales?
4. ¿El administrador del Sitio WEB, monitorea la actividad del mismo?
5. ¿Se utiliza la codificación de caracteres UTF-8?
6. ¿El municipio realiza mantenimiento y monitoreo de las herramientas de filtrado?
7. ¿Existe una declaración en términos claros y precisos respecto del tratamiento de los datos personales desde el sitio WEB, condiciones y garantías sobre confidencialidad del tratamiento de datos personales, derechos del usuario, en cuanto titular de los datos, para su debido resguardo?

CONCLUSIONES:

La auditoría deberá concluir si el municipio debe adoptar las medidas necesarias que permitan normalizar la estructura del departamento de informática, integrar personal al área de informática, especializar personal en áreas de seguridad informática e ingeniería de Software, adecuar el reglamento interno municipal para la estructura, organización y funciones informáticas a nivel general y específico.

Asimismo, se deberá adoptar medidas tendientes a evaluar técnica y profesionalmente al personal de informática, orientando a salvaguardar la

- Controles de Procedimientos de Respaldo
- Controles y procedimientos de recuperación de desastres
- Controles específicos asociados a las aplicaciones de procesos significativos.

Sistemas Administrativos Municipales

- ✓ Permisos de Circulación
- ✓ Patentes Comerciales
- ✓ Derechos de Aseo
- ✓ Contabilidad Gubernamental
- ✓ Tesorería Municipal

Contratos Vigentes

- ✓ Hosting y Mantención de WEB
- ✓ Servicios Telefónicos
- ✓ CAS Chile S.A. (Intranet Municipal)
- ✓ Servicios de Arriendo de Máquinas Fotocopiadoras
- ✓ Servicios Computacionales Área Administrativa.

Cumplimiento de los Decretos Supremos N°s:

- 77 del Ministerio Secretaría General de la Presidencia, sobre normas técnicas para la comunicación electrónica entre órganos públicos.-
- 81 del Ministerio Secretaría General de la Presidencia sobre interoperabilidad de documentos electrónicos
- 83 del Ministerio Secretaría General de la Presidencia Norma técnica sobre seguridad e interoperabilidad de documentos electrónicos
- 93 del Ministerio Secretaría General de la Presidencia , que aprueba la norma técnica para la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los órganos de la administración del Estado y sus funcionarios.

1. Personal Informático
2. Políticas de Sistema e Inversión de Equipamento
3. Matriz de Control Informático
4. Revisiones Programadas y Auditorías

b. Riesgos Asociados a TI:

1. **Obtención o Renovación Permisos de Circulación:** ¿Se tiene registro y/o acreditación física y online de datos del propietario, Placa Patente Única, Seguro Obligatorio, Revisión Técnica y Multas Impagas?
2. **Obtención o Renovación Patente Comercial:** ¿Se tiene registro y/o acreditación física de datos del contribuyente, propiedad, sucursales y Datos del Servicio de Impuestos Internos?
3. **Cálculo de derechos de Aseo de Contribuyentes Afectos.-**
4. **Recepción de Pagos con cálculo de intereses y multas fuera de período.-**
5. **Emisión de Cheques Individual con consulta de datos en sistema de contabilidad gubernamental.**
6. **Decretos de Pago imputados a cuentas presupuestarias que no corresponden.**

6.- Revisión de Contratos Asociados a TI:

7.- Controles Generales Asociados al Entorno TI:

1. **Controles Generales de Tecnología de Información:** Se debe comprobar que existan controles asociados a las tecnologías de información y que estos cumplan a cabalidad con el debido resguardo de la información verificando que el perfilamiento de accesos posea una asignación segregada de asignaciones de permiso impidiendo un incremento de cuentas que accedan a

7. Señalética.
8. Registro de Ingreso de personas, reparaciones de la plataforma de hardware y/o instalaciones que se realizan.-
9. Registro de mantenciones del aire acondicionado.

8.- Procedimientos de Respaldo

a. Verificar frecuencia y medios de respaldo.
b. Verificar existencia de encargado de respaldo de la información
c. ¿Se prueban regularmente los dispositivos de respaldo?
d. ¿Se realizan más de una copia de respaldo?

9.- Plan de Recuperación de Desastres:

a. Verificar la existencia de un plan de recuperación de desastre informático ante cualquier eventualidad.- este plan de recuperación debería contemplar existencia de medidas sobre evaluación de criticidad de procesos, alcance y descripción del plan a nivel anualidad, declaración de fallas, enfoque y tiempos de recuperación, grupo de contingencia, trabajo básico inter-áreas, y plan alternativo.

10.- Ejecución de Recorridos de Controles Generales Asociados a TI:

a. Sistemas Administrativos Municipales Incluidos Servicios Online.-

- Funciones: Se analizarán las funciones que realizan los sistemas administrativos municipales en relación con procesos significativos como:
  - Sistema de Contabilidad Gubernamental.
  - Sistema Derechos de Aseo
  - Sistema Tesorería Municipal
    - Egresos
    - Ingresos

g.- Control de Integridad: Verificar la existencia de controles de análisis de las bases de datos y que no exista, por ejemplo registros duplicados para un mismo valor numérico.

h.- Control de Reglas de Negocios: Verificar posibles errores en la asociación de pagos devengados con los centros de costo y/o programas relacionados.-

i.- Pruebas de Caja Negra: Tomando aleatoriamente un módulo, verificar que no se provoquen anomalías en los valores impresos.-

j.- Pruebas de Razonabilidad de Cifras Calculadas: Verificar aleatoriamente que los sistemas administrativos no presenten diferencias en las muestras respecto de los cálculos de valores.

k.- Revisión de Gestión de Cuentas de Sistemas Administrativo Municipales: Análisis base de datos "SQL Server?" y distintos módulos de estudio:

- Alcances al diseño lógico de base de datos
- Alcances a cuentas de acceso.

11.- Control de Cambios: Verificar que en los sistemas administrativos municipales exista un módulo de control de transacciones que consolide los movimientos propios de cada una de las aplicaciones como datos básicos relativos a cada una de las tablas.-

- Revisión de cambios en tabla Maestro de Proveedores del Sistema de Contabilidad Gubernamental.
- Consistencia o Inconsistencia del campo mprov_RUTprov
- Constatación de restricción de no nulo del campo mprov_dirprov, que representa la dirección del proveedor.
- Revisión de cambios en tabla de depósitos de sistema de tesorería municipal.-

solicitados, recibidos en las casillas electrónicas del Municipio asignadas a los distintos funcionarios.

La verificación será en los siguientes términos:

a. ¿El Municipio identifica y evalúa los riesgos y costos asociados a la recepción de mensajes electrónicos masivos no deseados?
b. ¿Se desarrollan, documentan o difunden políticas de uso, almacenamiento, acceso y distribución de mensajes electrónicos y de los sistemas informáticos utilizados en su procesamiento en documentación formal?
c. ¿Se realiza monitoreo del cumplimiento de los procedimientos establecidos, de manera de reducir los costos asociados a la recepción de mensajes masivos no deseados y que no guardan relación con el quehacer municipal?
d. ¿Se han instalado los sistemas informáticos adecuados para la filtración de mensajes masivos no deseados entrantes al servidor o servidor de correo?
e. ¿Se ha ofrecido en la página WEB un contacto para el encargado de informática?
f. ¿El Municipio, asegura un adecuado funcionamiento de las herramientas de filtrado, realizando mantenimiento de las mismas, con períodos de a lo menos 6 meses?

d.- Decreto Supremo N° 100 del año 2.006, del Ministerio Secretaría General de la Presidencia, que establece características mínimas obligatorias que deben cumplir los sitios WEB de los órganos de la Administración del Estado.- La auditoría se hará al siguiente tenor:

confidencialidad e integridad de los datos informáticos municipales e instruir la creación de procedimientos de seguridad informática.

CHRISTIAN MANUEL PARRA TORO

DIRECTOR DE CONTROL

MUNICIPALIDAD DE SAN PEDRO DE ATACAMA