MUNICIPALIDAD DE SAN JOAQUIN
DIRECCIÓN DE GESTION ADMINISTRACION

DECRETO Nº 136
Sección 1era.

SAN JOAQUÍN, 19 ENE 2016

LA ALCALDIA DE SAN JOAQUÍN, HOY DECRETO LO SIGUIENTE:

VISTOS: Informe N°61/2014 de la CGR; Ordinario 1300/45 de fecha 15.07.2015 de la Municipalidad de San Joaquín; Decreto N°83/2014 del Ministerio Secretaria General de la Presidencia que aprueba la norma técnica para los órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los documentos electrónicos."; Decreto Alcaldicio N°2269 de fecha 10.11.2015 que nombra encargado de Seguridad en materia de documentos electrónicos; Providencia de Administrador Municipal N° 67 de fecha 19.01.16,

TENIENDO PRESENTE: Las facultades que me confiere la Ley Nº 18.695, Orgánica Constitucional de Municipalidades, cuyo texto refundido fue fijado por el D.F.L.Nº 1 del Ministerio del Interior publicado en el Diario Oficial el 26 de julio del 2006.

DECRETO:

1.- Apruébese el Manual de Procedimiento del Departamento de Informática de la Municipalidad de San Joaquín de acuerdo a documento adjunto y al siguiente detalle:

- De los usuarios
- De la recepción de solicitudes
- De las cámaras de seguridad
- De los equipos nuevos
- Regulación de los procedimientos de las operaciones y administración de los sistemas informáticos de las empresas proveedoras
- Estructura y registro de incidencias de pérdidas de datos
- Procedimientos de control de cambios de sistemas
- Análisis de vulnerabilidad de la red local
- Procedimiento de mantención preventiva y correctiva de los equipos TIC
- Procedimiento de respaldo
- Procedimiento de eliminación de la información respaldada y revisión de las transacciones por sistema
- Procedimiento de control, utilizado para el acceso a la red, al sistema y a las aplicaciones.

ANÓTESE, COMUNÍQUESE, CÚMPLESE Y ARCHÍVESE.

ERIC LEYTON RIVAS
SECRETARIO MUNICIPAL

SERGIO ECHEVERRIA GARCIA
ALCALDE

MANUAL DE PROCEDIMIENTOS DEL DEPARTAMENTO DE INFORMATICA TI.

1. OBJETIVO

Determinar los diferentes procesos y responsabilidades que componen los servicios que presta el departamento de Informática de la Municipalidad de San Joaquín

2. DE LOS USUARIOS DE LA RED MUNICIPAL

2.1 La creación de usuarios se realizará a petición del Director (a), o Jefe de Departamento, o Unidad, o Sección cuando corresponda, por medio de un e-mail al Departamento de Informática, indicando nombre completo del funcionario, Departamento, Unidad o Sección en el cual se desempeñara.

El Departamento de Informática procederá a su creación de la siguiente manera:

- Se ingresa al Servidor de dominio, Active Directory, dominio San Joaquín, Dirección, Departamento, se crea al usuario: nombre y apellido y contraseña, la cual tendrá que cambiar al inicio sesión.

- Se procederá en igual manera a incorporar al grupo local y al firewall como usuario Restringido, Medio o Full según requerimiento.

2.2 El bloqueo o eliminación de usuarios de la red se realizara a petición del Director (a), o Jefe de Departamento, o Unidad, o Sección cuando corresponda, por medio de un e-mail al Departamento de Informática, indicando nombre completo del funcionario, Departamento, Unidad o Sección en el cual se desempeñaba, con el fin de bloquear o eliminar sus cuentas del dominio y correo municipal

El Departamento de Informática procederá a su bloqueo o eliminación de la siguiente manera:

- Se ingresa al Servidor de dominio, Active Directory, dominio San Joaquín, Dirección, Departamento, se bloquea o elimina al usuario.

Encargados responsables en el Departamento de Informática: Alejandro Adio

Gabriel Silva

Carlos Saavedra

3. DE LOS USUARIO DE CORREO INSTITUCIONAL

3.1 La creación de correo institucional para funcionario/usuarios se realizara a petición del Director (a), o Jefe de Departamento, o Unidad, o Sección cuando corresponda, por medio de un e-mail al Departamento de Informática, indicando nombre completo del funcionario, Departamento, Unidad o Sección en el cual se desempeñara.

El Departamento de informática procederá a su creación de la siguiente manera:

- Se ingresa al Servidor de Correo, se crea al usuario nombre apellido y contraseña.
- Se concurre al equipo que utilizara el (la) funcionario/usuarios, con el fin de configurar su cuenta en Outlook.
- Cumplido lo anterior, la cuenta queda habilitada.

3.2 La eliminación de usuario de correo se realizara a petición del Director (a), Jefe de Departamento, o Unidad, o Sección cuando corresponda, por medio de un e-mail al Departamento de Informática, indicando nombre completo del funcionario, Departamento, Unidad o Sección en la cual se desempeñaba.

- Se ingresa al servidor de correo y se procede a la eliminación de la cuenta institucional, además del descargo de la Libreta de Contactos Outlook, listado que se encuentra en el servidor: Publico /informática /Listado Usuarios Outlook para su incorporación o actualización en la Lista de contactos de Outlook.

Encargados responsables en el Departamento de Informática: Carlos Saavedra

Alejandro Adío

Gabriel Silva

3.3 Con el fin de mantener actualizada la Libreta de contactos, se realizará en forma periódica la revisión del personal municipal con contrato vigente, para lo anterior, se solicitará al Departamento de Recursos Humanos la nómina de funcionarios y personal honorarios, a fin de validar la existencia de correo institucional. Esta acción se realizará al menos en cada trimestre.

Encargados responsables en el Departamento de Informática: Ana María Bravo.

4. DE LA RECEPCÍON DE SOLICITUDES EMAIL, TICKET-SOPORTE, STOCK INSUMOS.

RECEPCION DE SOLICITUDES

4.1 Las solicitudes son recepcionadas por la asistente del Departamento de Informática TI, la cual procede a realizar el ticket-soporte (solicitudes tales como casillero.pst Outlook, equipo no enciende, encuadrado de Excel etc.) correspondiente, asignando a uno de los técnicos o especialistas del Departamento.

ENVIO DE CORREOS MASIVOS

4.2 El envío de correos masivos al grupo de usuarios/funcionarios de la Municipalidad de San Joaquín, sólo se tramita previa autorización del Administrador Municipal o Director (a) de la Dirección Gestión Administrativa.

MANTENCION DE INSUMOS COMPUTACIONALES

4.3 El control y mantención del stock de insumos computacionales (tóner, tintas, papel plotter, etc), se realiza previa proyección de los gastos de insumos en un período determinado, en conformidad a la demanda histórica y según fechas especiales de mayor consumo de productos. De acuerdo a lo anterior se gestiona solicitud de compra.

DE LOS REQUERIMIENTOS DE EQUIPAMIENTO O MEJORAS

4.4 En los casos de requerimiento de equipos computacionales, scanner u otros dispositivos, se procederá a la asignación de éstos previo registro de inventario y y configuración de usuario, si procede. De no existir stock en alguno de los casos, el Director de Gestión Administrativa evaluará la compra de equipamiento, para lo cual, se tramitará solicitudes de compra, según requerimiento. Cabe destacar que en el proceso de Permisos de Circulación las compras se encuentran proyectadas, debiendo proceder cada año con la compra de equipamiento que cumpla en forma satisfactoria con las necesidades que exige el proceso.

5. DE LAS CAMARAS DE SEGURIDAD CCTV

5.1 A solicitud de las Direcciones o Jefaturas se realizan búsquedas de eventos que afectaron la seguridad de los usuarios/funcionarios o instalaciones, o bien el requerimiento de revisar imágenes por una determinada importancia que pudiera significar esta evidencia en aquellos espacios de Municipalidad de San Joaquín, realizando respaldo de las grabaciones de dichos eventos.

6. DE LOS EQUIPOS NUEVOS

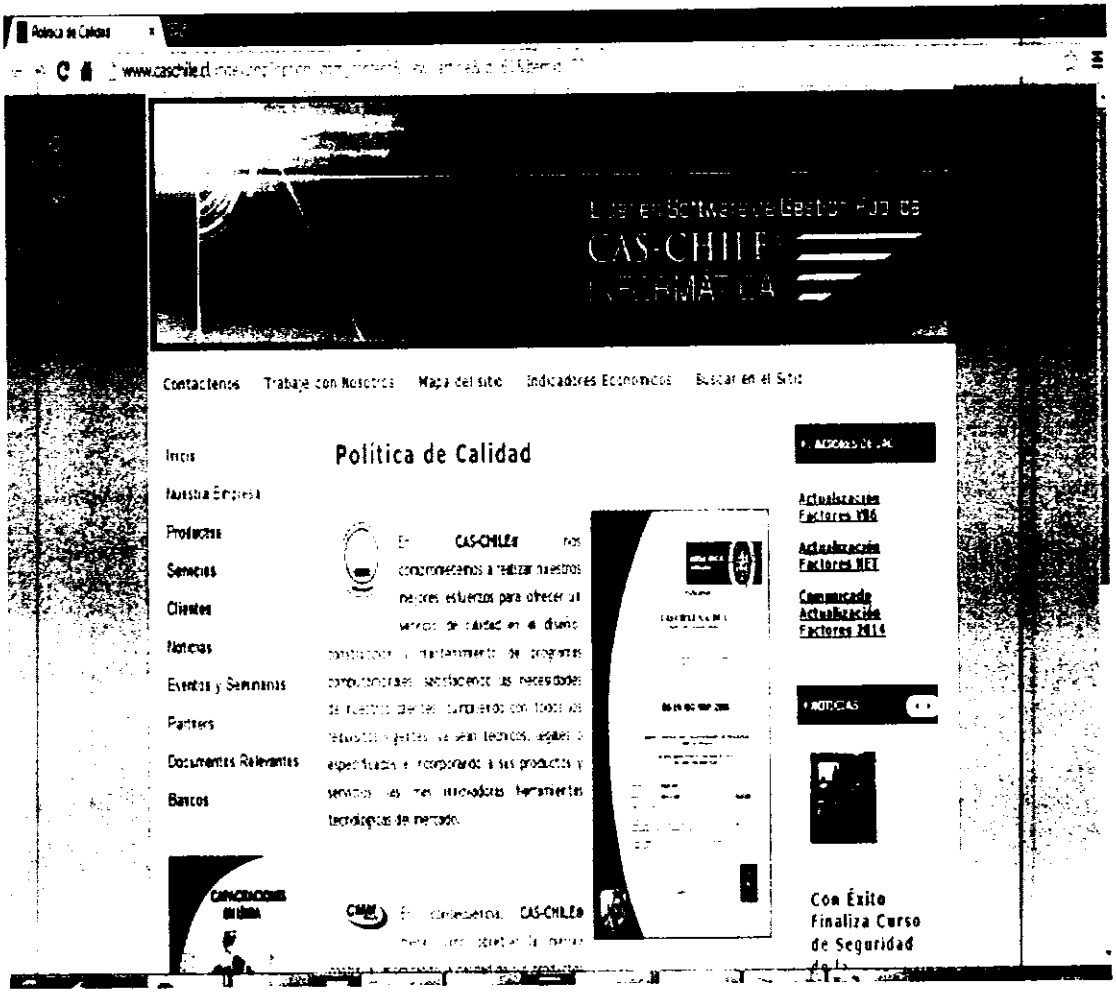
6.1 Los equipos tales como PC, Laptop (Notebook), Impresoras, Scanner, Monitores etc., se procede a registrarlos en su correspondiente hoja de vida, a continuación si corresponde se carga el sistema operativo (SO), su aplicación Ofimática, antivirus, actualización de SO, Ofimática. antivirus y software antimalware, quedando en stock para su posterior asignación por la Dirección DGA o Jefe del Departamento Informática TI

NOTA: según políticas de seguridad informática de Municipalidad de San Joaquín, todos los softwares que se adquieran deberán contar con sus respectivas licencias, aplica Ley 17.336

7. REGULACIÓN DE LOS PROCEDIMIENTOS DE LAS OPERACIONES Y ADMINISTRACIÓN DE LOS SISTEMAS INFORMÁTICOS DE LAS EMPRESAS PROVEEDORAS

El municipio cuenta con los instrumentos de control sobre las empresas proveedoras para el cumplimiento de los contratos, en virtud a los ***requerimientos técnicos y sistémicos*** de los sistemas de información, velando por el cumplimiento operacional de los contratos y/o servicios vigentes. Así también, son aplicables administrativamente las multas por incumplimiento del servicio.

Además, señalar la empresa que presta los servicios sobre los sistemas de información cuenta con una certificación ISO 9001:2008, "Diseño, construcción y Mantenimiento de programas computacionales", se adjunta a archivo, y publicación de su portal Web con fecha 12 de mayo 2014.



BUREAU VERITAS
Certification

Certification

Awarded to

CAS CHILE S.A. DE I.

[illegible] N° [illegible], Providencia - Santiago
CHILE

Bureau Veritas Certification certify that the Management System of the above organization has been assessed and found to be in accordance with the requirements of the standards detailed below

STANDARD

BS EN ISO 9001:2008

SCOPE OF SUPPLY

DISEÑO, CONSTRUCCION Y MANTENIMIENTO DE PROGRAMAS COMPUTACIONALES.

DESING, DEVELOPMENT AND MAINTENANCE OF COMPUTER SOFTWARE.

Audit date: **[illegible] 2010**

Original approval date: **March 21, [illegible]**   Certificate valid until date: **May 19, 2011**

Subject to the continued satisfactory operation of the organization's Management System

To check this certificate validity please call [illegible].
Further clarifications regarding the scope of this certificate and the applicability of the Management System requirements may be obtained by consulting the organization.

Certificate Number: [illegible]   Date: [illegible]
Number Review: 01

[illegible]
General Manager

8. ESTRUCTURA Y REGISTRO DE INCIDENCIAS DE PÉRDIDAS DE DATOS

1.- Objetivo

Describir las actividades de ser necesarios en las incidencias de pérdida de datos de los sistemas disponibles e implementados en la Municipalidad de San Joaquín. Ante la posibilidad de una incidencia mayor el municipio cuenta con los respaldos de sus bases de datos y /o aplicaciones, disponibles de las empresa que presta los servicios de nuestros sistemas.

2. Alcance

Para mitigar ante la eventualidad de sufrir una incidencia de los sistemas por pérdida de datos, se indica los mecanismos disponibles, que resguarda la información de los sistemas como así asegurar los respaldos que se encuentran disponibles. Con la finalidad de salvaguardar los datos e información del municipio.

3.- Responsabilidades

La responsabilidad del Departamento de informática y/ó la empresa que presta los servicios en resguardar la información de los sistemas de Información, los que deben realizar los respaldos periódicos de los sistemas y bases de datos, de cada uno de ellos.

4.- Procedimientos de recuperación de incidencias de datos

4.1.- Cambio de versión y/o actualización de los sistemas

Ante la eventualidad que en producción exista una pérdida de datos, provocado por la instalación de una nueva línea base y/o la actualización de una nueva versión de los sistemas de información, se indica los pasos que son aplicables en este escenario:

	Actividad (Diagrama de Flujo)	Descripción de la actividad	Responsable	Documento o Registro
Restauración de datos por incidencia de cambio actualización de los sistemas				
	Inicio	**Inicio del procedimiento**		
1	**Registro** de la nueva línea en producción	Se debe realizar los ***respaldos*** de los sistemas y/o tablas de las bases de datos	soporte de la empresas que presta los servicios	Se debe ejecutar el procedimiento de ***plan de respaldo*** (respaldo de base de datos y/o Línea base previo al instalación)
2	***Reporte de incidencia*** de pérdida de datos por actualización de los sistemas	Se debe adjuntar los datos y/o registros que genera la incidencia de pérdida de datos	Encargado y/o Jefe de la unidad	Envio y registro de los eventos de pérdida de los datos
3	***Carga de línea base*** previo a la incidencia	Se debe ejecutar y realizar los respaldos de las bases de datos previo a la instalación, realizada en el punto uno.	Departamento de Informatica y/o soporte de la empresas que presta los servicios	Registrar e informar a los encargados y/o Jefe de áreas que se ejecuta correctamente la carga de los datos previo a la instalación de la nueva versión
4	Verificación & Validación	El funcionario municipal ó el funcionario a contrata será el responsable de realizar las pruebas y validación de las correcciones aplicadas	Encargado del área & Encargado del departamento de Informatica	Realizar las pruebas de validación
	Fin	Fin del procedimiento		

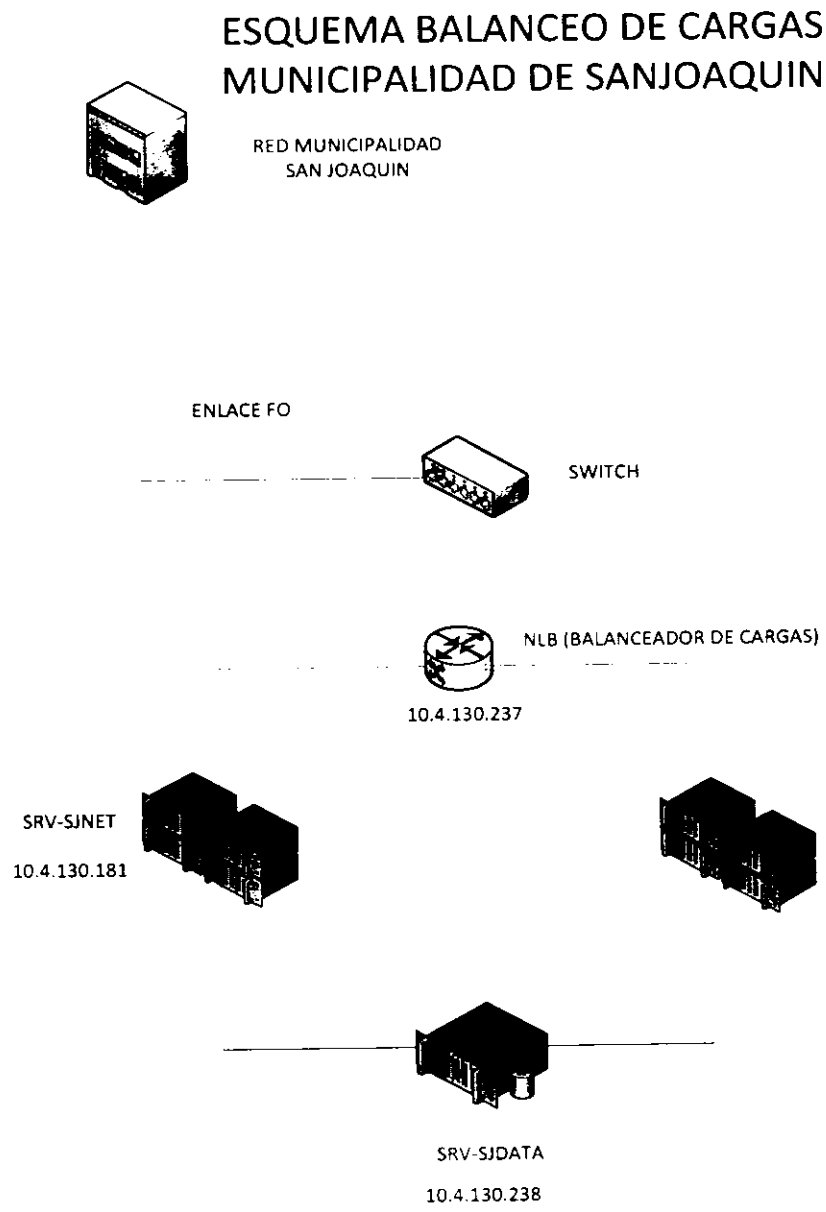
4.2.- Incidencia por alteración en el funcionamiento de los sistemas

Tiene por objetivo registrar las incidencias reportadas sobre los sistemas que afectan su normal funcionamiento.

	Actividad (Diagrama de Flujo)	Descripción de la actividad	Responsable	Documento o Registro
Reporte de Problemas				
	Inicio	**Inicio del procedimiento**		
1	Identificar el Reporte de Problemas	Se determinan e identifican el Reporte de Problemas indicado por el o los funcionarios municipales	Encargado de Informatica & soporte Cas chile	
2	Elaboración del ***RP*** (Reporte de Problemas)	Registra la incidente notificado por el usuario del sistema de información y lo canaliza al personal de Soporte.	Encargado de Informatica y/o quien lo subrogue	Elaboración del documento ó email con el reporte de problemas del sistema
3	***Notificación***	Elaborar los ***RP*** (Reporte de Problemas a la empresa que presta los servicios	Soporte de empresa contratista	Elaboración del documento ó email con el RP, al Jefe de Proyecto
4	Desarrollo	Corregir el reporte de problema si aplica a procedimiento almacenado, trigguer, etc, ó sobre el sistema (.NET y/o Visual)	Soporte, DBA, Webmaster de sistemas de empresa contratista	Enviar las fechas de los entregables (por contrato no debe superar los 3 días)
5	Liberar	Se debe liberar línea base	Soporte de empresa contratista	Enviar y notificar la disponibilidad de los sistemas en él a los funcionarios responsables de la solicitud de cambio Se debe enviar el ***V°B°*** con la aprobación de la nueva línea base
6	Generar los respaldo de los sistema y las bases de datos del servidor de producción	Realizar y programar el respaldo de las bases de datos y la línea base	Soporte de empresa contratista	Aplicar el procedimiento de respaldo de datos
7	Verificación & Validación	El funcionario municipal ó el funcionario a contrata será el responsable de realizar las pruebas y validación de las correcciones aplicadas	Encargado del área & Encargado del departamento de Informatica	Realizar las pruebas de validación
	Fin	Fin del procedimiento		

4.3.- Estructura & diagrama del balanceador de carga para los sistemas de Cas-Chile para el funcionamiento de los sistemas

Se adjunta el diagrama y estructura física de los balanceadores de carga y el servidor de respaldo aplicados sobre las bases de datos de los sistemas de información de Cas Chile, para el correcto funcionamiento de los sistemas.



9. PROCEDIMIENTOS DE CONTROL DE CAMBIOS SISTEMAS

1.- Objetivo

Describir las actividades de administrar y/ó controlar los cambios realizados a los Sistemas de Información de los sistemas de Caschile y/o a sistemas operativos implementados en la municipalidad de San Joaquín, manteniendo los niveles de autorización y documentación pertinentes.

2. Alcance

El presente procedimiento es de aplicación para todos los sistemas y los procesos y que requieran solventar inconsistencias, nuevos requerimientos y cambios en los sistemas.

3.- Procedimientos y/o Documentos relacionados

3.1.- Responsabilidades

El encargado del departamento Informatica y/o quien lo subrogue es responsable de asegurar que el Procedimiento de Control de Cambios y Liberaciones de una nueva versión de los Sistemas de Información se cumpla en todos sus pasos, cumpliendo con la versión vigente y con los nuevos controles de cambios solicitados, proporcionando satisfacción a los usuarios en la resolución de un incidente.

3.2.- Responsabilidades Proveedor/Desarrollador

El Jefe de proyecto de la empresa que presta los servicios y/o quien lo subrogue es el responsable de realizar las modificaciones al sistema para dar solución a las inconsistencias detectadas, así como a los nuevos requerimientos y cambios solicitados por el departamento de y/o dirección solicitante, cumpliendo con las normatividad vigente y con la nueva versión quede operativa y sin reporte de problemas, de lo contrario es responsabilidad de la empresa que presta los servicios.

3.3.- Descripción del procedimiento

Actividad (Diagrama de Flujo)		Descripción de la actividad	Responsable	Documento o Registro
Requerimiento con Control de Cambio				
	Inicio	**Inicio del procedimiento**		
1	Solicitud de control de Cambio y/o Requerimiento	Se determinan e identifican los archivos a respaldar en los equipos en las diferentes áreas.	Encargado de Informatica & soporte de empresa contratista	
2	Elaboración del ***SR*** (Requerimientos de Software)	Se identifica el o las pantallas de sistema que afectan al sistema, para los nuevos controles de cambio solicitados	Encargado de Informatica y/o quien lo subrogue	Elaboración del documento ó email con el SR para el nuevo requerimiento
3	Elaboración del ***SR*** (INTERNO)	Elaborar los ***SR***, internos con los controles de cambios solicitados	Soporte de empresa contratista	Elaboración del documento ó email con el SR, a los Jefe de Proyecto (de la municipalidad y empresa que presta los servicios)
4	Desarrollo	Desarrollo del nuevo requerimiento del sistema	Soporte, DBA, Webmaster de sistemas de empresa contratista	Enviar las fechas de los entregables (por contrato no debe superar los 15 días)
5	Instalación de la Linea Base y la carga de datos en el servidor de Prueba y equipos de prueba	Se debe liberar linea base en el servidor de prueba	Soporte de empresa contratista	Enviar y notificar la disponibilidad de los sistemas en el ambiente de prueba a los funcionarios responsables de la solicitud de cambio
6	Verificación & Validación de la Nueva Linea Base del Sistema	El funcionario municipal ó el funcionario a contrata será el responsable de realizar las pruebas y validación de los nuevos requerimiento	Jefe de la unidad solicitante y/o Encargado del área	Realizar las pruebas de validación del control de cambio solicitado Se debe enviar el V°B° con la aprobación de la nueva linea base
7	Generar los respaldo de los sistema y las bases de datos del servidor de producción	Realizar y programar el respaldo de las bases de datos y la linea base	Soporte de empresa contratista	Aplicar el procedimiento de respaldo de datos
8	Instalación en Producción	Se debe notificar por escrito y/o correo al encargado del departamento de Informatica, para la liberación de la nueva línea base aprobada por el encargado del departamento y/o unidad solicitante	Soporte de empresa contratista	Se debe señalar el cambio de versión anterior y la nueva versión
9	Verificación & Validación la nueva linea base del Sistema	El funcionario municipal ó el funcionario a contrata encargado será el responsable de realizar las pruebas y validación de los nuevos requerimiento	Jefe de la unidad y/o Encargado del área del solicitante	Se debe enviar el V°B° con la aprobación de la nueva linea base Encargado de informática y al Jefe de la Unidad
Fin		Fin del procedimiento		

Actividad (Diagrama de Flujo)		Descripción de la actividad	Responsable	Documento o Registro
Reporte de Problemas				
	Inicio	**Inicio del procedimiento**		
1	Identificar el Reporte de Problemas	Se determinan e identifican el Reporte de Problemas indicado por el o los funcionarios municipales	Encargado de Informatica & soporte Cas chile	
2	Elaboración del ***RP*** (Reporte de Problemas)	Registra la incidente notificado por el usuario del sistema de información y lo canaliza al personal de Soporte a Sistemas de Información.	Encargado de Informatica y/o quien lo subrogue	Elaboración del documento ó email con el reporte de problemas del sistema
3	Notificación	Elaborar los ***RP*** (Reporte de Problemas a la empresa que presta los servicios	Soporte de empresa contratista	Elaboración del documento ó email con el RP, al Jefe de Proyecto
4	Desarrollo	Corregir el reporte de problema si aplica a procedimiento almacenado, trigguer, etc, ó sobre el sistema (.NET y/o Visual)	Soporte, DBA, Webmaster de sistemas de empresa contratista	Enviar las fechas de los entregables (por contrato no debe superar los 3 días)
5	Liberar	Se debe liberar línea	Soporte de empresa contratista	Enviar y notificar la disponibilidad de los sistemas en el a los funcionarios responsables de la solicitud de cambio Se debe enviar el ***V°B°*** con la aprobación de la nueva línea base
6	Generar los respaldo de los sistema y las bases de datos del servidor de producción	Realizar y programar el respaldo de las bases de datos y la línea base	Soporte de Cashile	Aplicar el procedimiento de respaldo de datos
7	Verificación & Validación	El funcionario municipal ó el funcionario a contrata será el responsable de realizar las pruebas y validación de las correcciones aplicadas	Encargado del área & Encargado del departamento de Informatica	Realizar las pruebas de validación
Fin		Fin del procedimiento		

10. ANÁLISIS DE VULNERABILIDAD DE LA RED LOCAL

1.- Objetivo

Identificar las vulnerabilidades a nivel de hardware disponibles en el municipio, a contar del levantamiento de la información.

2. Plan de mitigación para la red local

Se debe realizar un plan de mejora en la red local y certificar nuestra red local a categoría 5e o superior, además de considerar la renovación de los equipamiento de **switch** y/o **router** como mínimo de switch de 24 puertos con alimentación POE, como parte de un plan de renovación del equipamiento computacional producto del ciclo de vida de los equipos y considerar el plan de expansión de los puntos de red y migración a telefonía IP, se debe considerar equipos nuevos con políticas de enrutamiento de última generación en los router y switch con Calidad de servicios(QoS) para priorización de tráfico.

3.- Escenario actual

Los routers disponibles, cumplieron su ciclo de vida, el cableado existente es de categoría 5 y/o inferior, se debe proceder a certificar la red.

- Los routers y switch existentes se deben renovar por equipos de nueva generación, que optimizan las políticas de enrutamiento de los datos.
- Eliminar la topología de red modelo cascada de algunos departamentos.

3.- Escenario esperado

- Mejorar el modelo de red local.
- Certificar la red a categoría 5e o superior.
- Adquisición de routers con Calidad de Servicio (QoS) para priorización de tráfico, puertos POE, autoadministrados y funciones de ahorro de energía.

11. PROCEDIMIENTOS DE MANTENCIÓN PREVENTIVA Y CORRECTIVA DE LOS EQUIPOS COMPUTACIONALES DE LA MUNICIPALIDAD DE SAN JOAQUÍN

OBJETIVO

Permitiendo administrar eficientemente los recursos asignados, convirtiéndose en una herramienta de apoyo a la gestión de mantención y con el fin de mantener los equipos informáticos actualizados y en óptimas condiciones, además de la seguridad informática para los funcionarios/usuarios de la Municipalidad de San Joaquín, se hace necesario contar con el siguiente procedimiento:

1. DE LA MANTENCION

1.1 MANTENCION PREVENTIVA.

Se deberá realizar la mantención preventiva cada seis (6) meses de los equipos utilizados por los funcionarios/usuarios de la Municipalidad de San Joaquín, teniendo como pauta los siguientes puntos:

- Limpieza interna del equipo PC, con soplador de alta potencia, además de brocha para sector de difícil acceso.
- Limpieza externa del equipo, con líquido especial para ello, así como paño de limpieza adecuado y otros utensilios.
- Actualización Sistema Operativo, dependiendo de la versión que el equipo cuente.
- Actualización Base Antivirus, al día que se realizara la mantención. Además se deberá verificar la tarea de planificación de la base antivirus para que ésta se realice dentro del horario de oficina.
- Actualización software utilitario.
- Eliminación de programas o software no autorizados, dejando constancia en el acta misma de las irregularidades detectadas e informar al Encargado de Seguridad del Departamento Informática para que adopte las medidas correspondientes.

- Limpieza de archivos temporales, tanto en la sesión del usuario como en la del administrador del equipo.
- Ejecutar programa "Liberador de Espacio en Disco" y posteriormente eliminar archivos señalados en programa.
- Reiniciar equipo e ingresar en "modo seguro" (F8) para posteriormente ejecutar software antivirus.
- Registrar los archivos infectados, si es que hubieran.
- Desfragmentación del Disco Duro.
- Completar ficha técnica del equipo para la firma del usuario. Esta ficha será confeccionada por el departamento de informática.

En cuanto a la mantención preventiva de los equipos Servidores, router, switch, impresión o scanner, ésta consistirá solo en limpieza exterior e interior.

CALENDARIO DE MANTENCIONES PREVENTIVAS SEMESTRALES

Primer Semestre: Enero Junio

Segundo Semestre: Julio Diciembre

1.2 MANTENCION CORRECTIVA.

Mantención que se realiza a petición del usuario, previo llamado telefónico o e-mail al Departamento de informática, por un mal funcionamiento del equipo a cargo. Una vez solucionado el problema, se deberá llenar la ficha técnica correspondiente la que será firmada por el usuario dando conformidad al acto.

Si el error presentado por el equipo no es solucionable, salvo el formateo del mismo, éste será retirado del lugar de trabajo y llevado al Departamento de Informática para su proceso, contando para ello de dos (2) días hábiles para la entrega. En caso de contar con equipo de reemplazo, se le instalara al usuario un equipo para que pueda seguir cumpliendo con su trabajo habitual hasta que le sea devuelto el equipo. Se deja claramente establecido que en caso de ser entregado un equipo en forma temporal éste sólo contara con lo necesario para cumplir con el trabajo habitual, no quedando instalado el correo institucional, el cual solo podrá ser visto vía web.

Si la información no es posible de ser recuperada, por desperfecto del disco duro del equipo, será responsabilidad del usuario el haber realizado el respaldo de ésta, en la unidad virtual creada en el servidor para este fin, tal como lo señala la Política se Seguridad. En lo que tiene relación con el correo institucional, la información no podrá ser recuperada, ya que en la actualidad no se hacen respaldos de los correos a nivel de servidor de correo.

Una vez formateado el equipo, realizado la limpieza exterior e interior, instalado los programas utilitarios, configurado el correo institucional e instaladas las actualizaciones correspondientes, el equipo será entregado al usuario, previa firma de la ficha correspondiente.

En cuanto a la mantención correctiva de los equipos Servidores, Router, Switch, impresión o scanner, ésta será realizada por el Servicio Técnico a fin, siendo retirado el equipo de la Dirección o Departamento o Unidad o Sección cuando corresponda.

De existir garantías se llevaran a efecto de inmediato, coordinando este trabajo la asistente del Departamento de Informática TI.

En el caso de mantenimiento de servidores, se realizan revisiones periódicas del funcionamiento, a fin de mantener las condiciones de operatividad de este elemento.

En cuanto al registro de fallas reales y sospechosas, se cumple con la revisión, según sea el caso de cada usuario afectado, todo lo anterior en estricta relación con las políticas de seguridad, software antivitus entre otros, con el fin de mantener los resguardos necesarios.

12. PROCEDIMIENTO DE RESPALDOS

1.- Objetivo

Describir las actividades que se realizan para efectuar el respaldo de la información relevante y pertinente de cada uno de los departamentos o áreas de la Municipalidad de San Joaquín.

Por las razones antes mencionadas es que se ha implementado un método sistémico que permite realiza los respaldos de los recursos compartidos del servidor público (intranet) y los respaldos diarios de las bases de datos, de la empresa que presta los servicios de nuestros sistemas.

2. Alcance

Iniciar con la programación que se tiene definida en el área de sistemas para las copias de seguridad de la información y bases de datos para salvaguardia la información.

3.- Procedimientos y/o Documentos relacionados

3.1.- Responsabilidades

La responsabilidad por el cumplimiento del procedimiento recae sobre los Jefes, directores de Departamentos y los funcionarios autorizados para el acceso a los sistemas y a los recursos compartidos de las carpetas del servidor de la Intranet, con los perfiles de acceso solicitados por la Jefatura estos son: lectura, escritura y/ó lectura / escritura. Para acceder a los recursos compartidos y a los sistemas esta debe ser canalizado mediante un memo interno o correo electrónico al departamento de Informática con copia al Jefe de departamento de Informatica y Jefe de Proyecto de Cas Chile, si procede. para el acceso a los sistemas y/ó al acceso a los carpetas del servidor de la Intranet.

Las jefaturas, funcionario, personal a contrata y/ó honorario, que son trasladada a otra unidad ó departamento se debe informar esta por intermedio de un memo, ó correo electrónico del Jefe directo informando el traslado al departamento de informática, para proceder con las modificaciones de privilegios de acceso a los sistemas, acceso al público (intranet). De lo contrario es responsabilidad del funcionario él no comunicar las modificaciones a los sistemas y/o recursos compartidos.

Los alumnos en práctica y en general los usuarios que utilicen o manipulen información se debe informar la confidencial o de importancia de la información que disponen los sistemas, lo que debe ser comunicado por el supervisor directo quien será el responsable de supervisar y verificar la manipulación de los datos sobre los sistemas, conforme a los perfiles de acceso solicitados para los sistemas.

3.2.- Descripción del procedimiento

Actividad (Diagrama de Flujo)		Descripción de la actividad	Responsable	Documento o Registro
Realización de Backup				
	Inicio	**Inicio del procedimiento**		
1	Determinar proceso de Backup	Se determinan e identifican los archivos a respaldar en los equipos en las diferentes áreas.	Departamento de Informatica	
2	Identificar aplicativos y/o base de datos	Se identifica el número de aplicativos y/o bases de datos para respaldo.	Departamento de Informatica & soporte Caschile	Inventario de aplicativos
3	Determinar mecanismos	Se determinan los mecanismos de copias de respaldo según la base de datos a respaldar de forma manual.	Departamento de Informatica & Soporte Caschile	Bitácora de backup
4	Verificar archivos	Se verifican los archivos log del aplicativo utilizado para la copia de seguridad.	Departamento de Informatica & soporte Caschile	
5	Verificar copias de restauración	Se verifican las copias para la restauración cuando se necesiten por cualquier usuario de la entidad.	Departamento de Informatica & soporte Caschile	
6	Realizar copia por segunda vez (Solicitado)	Si el archivo log del servidor indica un error, se realiza copia por segunda vez.	Departamento de Informatica	
7	Grabar copias	Se graba de manera diaria, semanal, mensual y anualmente de acuerdo con la política de backup, en un dispositivo de almacenamiento (Disco Externo) todas las copias y guardada en el servidor y disco externo en el departamento de Informatica.	Departamento de Informatica	
8	Almacenar copia (Solicitadas)	Se almacena la copia, y para el caso de ser un medio magnético (CD y/o DVD) se marca con la respectiva fecha, usuario y nombre del equipo	Departamento de Informatica & soporte Caschile	
Fin		Fin del procedimiento		

Actividad (Diagrama de Flujo)		Descripción de la actividad	Responsable	Documento o Registro
Restauración				
	Inicio	**Inicio del procedimiento**		
1	Determinar aplicativos y/o base de datos	Se determina o identifica el número de aplicativos y/o bases de datos para la restauración.	Departamento de Informatica	
2	Realizar restauración	Se realiza la restauración de los archivos correspondientes en el equipo del usuario. Si es una base de datos, se determina la hora para la respectiva restauración y se informa a los usuarios para suspender el Aplicativo mientras se realiza la respectiva reposición.	Departamento de Informatica & soporte Caschile	Inventario de aplicativos
3	Registrar restauración	Se determinan los mecanismos de copias de respaldo según la base de datos a respaldar de forma manual.	Departamento de Informatica	Bitácora de Backup
Fin		Fin del procedimiento		

13. PROCEDIMIENTOS DE ELIMINACIÓN DE INFORMACIÓN RESPALDADA Y REVISIÓN DE LAS TRANSACCIONES POR SISTEMA

1.- Objetivo

Describir las actividades de controlar para el Procedimientos de eliminación de Información respaldada y revisión de las Transacciones por sistema, que se soliciten al departamento de Informatica.

2. Alcance

El presente procedimiento describe las actividades y tareas que se debe aplicar a todos los sistemas y los procesos que deben ser aplicables sobre los sistemas.

3.- Procedimientos y/o documentos relacionados

3.1.- Responsabilidades

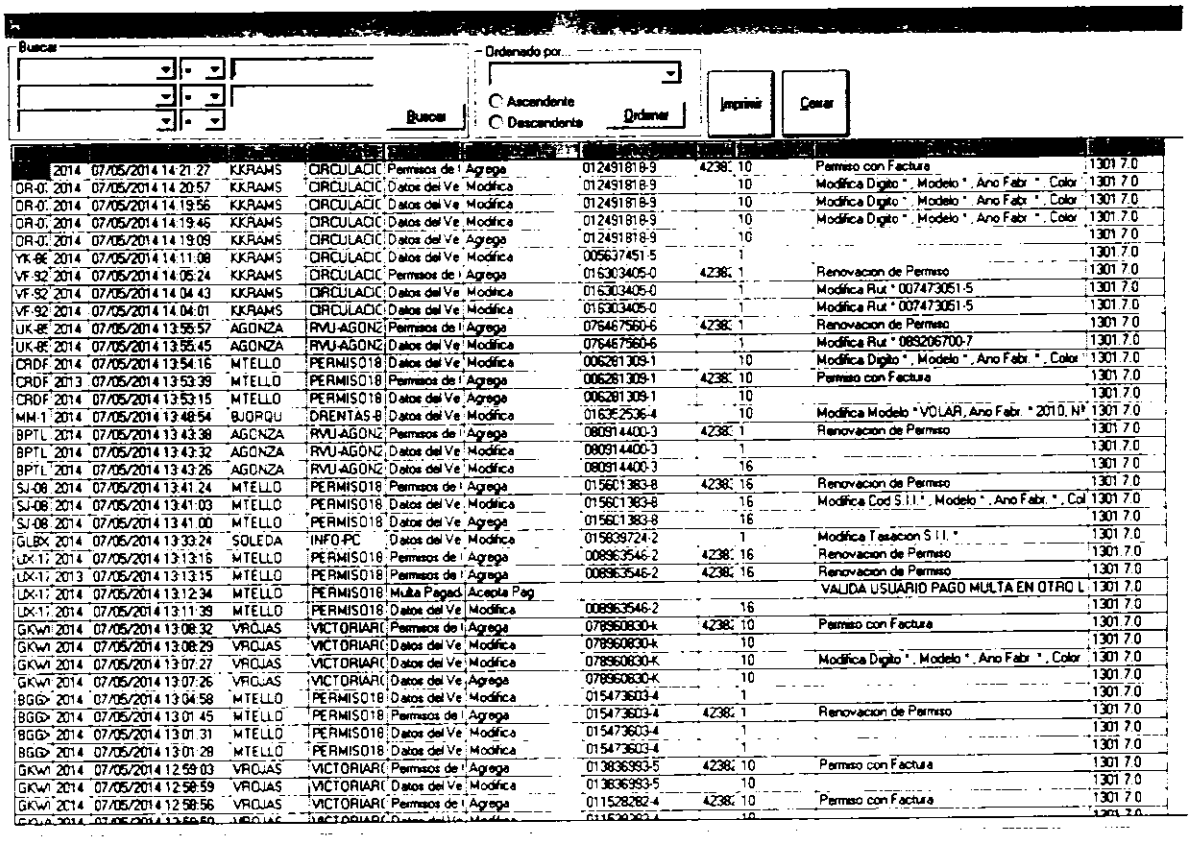
Aplica el procedimiento solo a la eliminación de información respaldada, quien será de responsabilidad el Jefe y/o supervisor del departamento que solicita la eliminación de la información respaldad sobre sus sistemas, quien debe informar y enviar un documento administrativo ***memo, providencia*** que apruebe la *eliminación de la Información respaldada* que luego debe ser validada y firmado por su Director directo, quien aprueba la eliminación de la información respaldada desde el sistema que será enviada al encargado del Departamento de Informática para su ejecución.

4.- Descripción del procedimiento

Actividad (Diagrama de Flujo)		Descripción de la actividad	Responsable	Documento o Registro
Procedimiento de Eliminación de Información Respaldada				
	Inicio	**Inicio del procedimiento**		
1	Solicitud de la eliminación de la Información Respaldada	Se determinar e identifican los archivos y/o registros de las bases de datos a aplicar.	Jefe / Supervisor del Área	
2	Elaborar documento administrativo para proceder con la eliminación	Elaborar memo, providencia y/o documento administrativo. Se debe indicar el ó los registros con la eliminación	Jefe / Supervisor del Área	Memo, providencia, con la solicitud de eliminación de ***información respaldada***
3	Verificación y Validación del documento administrativo	Se debe validar y verificar la información que se requiere para eliminar la ***información respaldada***	Director / Jefe a cargo	Certificar y aprobar solicitud adjunta
4	Comprobar los respaldo de los sistema y los registros	Realizar y programar el respaldo de las bases de datos y la línea base	Departamento de Informatica y/o Soporte de empresa contratista	Aplicar el procedimiento de respaldo de datos
5	Verificar y Validar los registros solicitados para la eliminación de la Información Respaldada	Se debe validar y verificar la información que se requiere para eliminar la ***información respaldada***	Encargado del Departamento de Informatica y/ó quien lo subrogue	Certificar y aprobar solicitud adjunta
5	Ejecutar el documento administrativo con la *eliminación de la información respaldada*	El funcionario municipal ó el funcionario a contrata encargado será el responsable de ejecutar memo, providencia de los registros solicitados	Departamento de Informatica y/o Soporte de empresa contratista	Se debe enviar el V°B° con la ejecución del procedimiento al Encargado de Informática y al Jefe de la Unidad
Fin		Fin del procedimiento		

5.- Revisión de las Transacciones por sistema

Los sistemas cuentan con unos registros de transacciones de los eventos con las transacciones que cada usuario realiza sobre el sistema, el perfil de acceso sobres estos registros es aplicable solo de consulta e impresión de la consulta solicitada por el usuario, esta puede ser en Excel y en un archivo pdf no modificable.



	2014	07/05/2014 14:21:27	KKRAMS	CIRCULACIC	Permisos de I	Agrega	012491818-9	4238 10	Permiso con Factura 1301 7.0
DR-0:	2014	07/05/2014 14:20:57	KKRAMS	CIRCULACIC	Datos del Ve	Modifica	012491818-9	10	Modifica Digito *, Modelo *, Ano Fabr. *, Color 1301 7.0
DR-0:	2014	07/05/2014 14:19:56	KKRAMS	CIRCULACIC	Datos del Ve	Modifica	012491818-9	10	Modifica Digito *, Modelo *, Ano Fabr. *, Color 1301 7.0
DR-0:	2014	07/05/2014 14:19:46	KKRAMS	CIRCULACIC	Datos del Ve	Modifica	012491818-9	10	Modifica Digito *, Modelo *, Ano Fabr. *, Color 1301 7.0
DR-0:	2014	07/05/2014 14:19:09	KKRAMS	CIRCULACIC	Datos del Ve	Agrega	012491818-9	10	1301 7.0
YK-86	2014	07/05/2014 14:11:08	KKRAMS	CIRCULACIC	Datos del Ve	Modifica	005637451-5	1	1301 7.0
VF-92	2014	07/05/2014 14:05:24	KKRAMS	CIRCULACIC	Permisos de I	Agrega	016303405-0	4238 1	Renovacion de Permiso 1301 7.0
VF-92	2014	07/05/2014 14:04:43	KKRAMS	CIRCULACIC	Datos del Ve	Modifica	016303405-0	1	Modifica Rut * 007473051-5 1301 7.0
VF-92	2014	07/05/2014 14:04:01	KKRAMS	CIRCULACIC	Datos del Ve	Modifica	016303405-0	1	Modifica Rut * 007473051-5 1301 7.0
UK-85	2014	07/05/2014 13:55:57	AGONZA	RVU-AGONZ	Permisos de I	Agrega	076467560-6	4238 1	Renovacion de Permiso 1301 7.0
UK-85	2014	07/05/2014 13:55:45	AGONZA	RVU-AGONZ	Datos del Ve	Modifica	076467560-6	1	Modifica Rut * 089206700-7 1301 7.0
CRDF	2014	07/05/2014 13:54:16	MTELLO	PERMISO18	Datos del Ve	Modifica	006281309-1	10	Modifica Digito *, Modelo *, Ano Fabr. *, Color 1301 7.0
CRDF	2013	07/05/2014 13:53:39	MTELLO	PERMISO18	Permisos de I	Agrega	006281309-1	4238 10	Permiso con Factura 1301 7.0
CRDF	2014	07/05/2014 13:53:15	MTELLO	PERMISO18	Datos del Ve	Agrega	006281309-1	10	1301 7.0
MM-1	2014	07/05/2014 13:48:54	BJORQU	DRENTAS-B	Datos del Ve	Modifica	016362536-4	10	Modifica Modelo *VOLAR, Ano Fabr. *2010, N° 1301 7.0
BPTL	2014	07/05/2014 13:43:38	AGONZA	RVU-AGONZ	Permisos de I	Agrega	080914400-3	4238 1	Renovacion de Permiso 1301 7.0
BPTL	2014	07/05/2014 13:43:32	AGONZA	RVU-AGONZ	Datos del Ve	Modifica	080914400-3	1	1301 7.0
BPTL	2014	07/05/2014 13:43:26	AGONZA	RVU-AGONZ	Datos del Ve	Modifica	080914400-3	16	1301 7.0
SJ-08	2014	07/05/2014 13:41:24	MTELLO	PERMISO18	Permisos de I	Agrega	015601383-8	4238 16	Renovacion de Permiso 1301 7.0
SJ-08	2014	07/05/2014 13:41:03	MTELLO	PERMISO18	Datos del Ve	Modifica	015601383-8	16	Modifica Cod S.I.I. *, Modelo *, Ano Fabr. *, Col 1301 7.0
SJ-08	2014	07/05/2014 13:41:00	MTELLO	PERMISO18	Datos del Ve	Agrega	015601383-8	16	1301 7.0
GLBX	2014	07/05/2014 13:33:24	SOLEDA	INFO-PC	Datos del Ve	Modifica	015639724-2	1	Modifica Tasacion S.I.I. * 1301 7.0
LDX-17	2014	07/05/2014 13:13:16	MTELLO	PERMISO18	Permisos de I	Agrega	008963546-2	4238 16	Renovacion de Permiso 1301 7.0
LDX-17	2013	07/05/2014 13:13:15	MTELLO	PERMISO18	Permisos de I	Agrega	008963546-2	4238 16	Renovacion de Permiso 1301 7.0
LDX-17	2014	07/05/2014 13:12:34	MTELLO	PERMISO18	Multa Pagad	Acepta Pag			VALIDA USUARIO PAGO MULTA EN OTRO L 1301 7.0
LDX-17	2014	07/05/2014 13:11:39	MTELLO	PERMISO18	Datos del Ve	Modifica	008963546-2	16	1301 7.0
GKWI	2014	07/05/2014 13:08:32	VROJAS	VICTORIAR(	Permisos de I	Agrega	078960830-k	4238 10	Permiso con Factura 1301 7.0
GKWI	2014	07/05/2014 13:08:29	VROJAS	VICTORIAR(	Datos del Ve	Modifica	078960830-k	10	1301 7.0
GKWI	2014	07/05/2014 13:07:27	VROJAS	VICTORIAR(	Datos del Ve	Modifica	078960830-K	10	Modifica Digito *, Modelo *, Ano Fabr. *, Color 1301 7.0
GKWI	2014	07/05/2014 13:07:26	VROJAS	VICTORIAR(	Datos del Ve	Agrega	078960830-K	10	1301 7.0
BGGX	2014	07/05/2014 13:04:58	MTELLO	PERMISO18	Datos del Ve	Modifica	015473603-4	1	1301 7.0
BGGX	2014	07/05/2014 13:01:45	MTELLO	PERMISO18	Permisos de I	Agrega	015473603-4	4238 1	Renovacion de Permiso 1301 7.0
BGGX	2014	07/05/2014 13:01:31	MTELLO	PERMISO18	Datos del Ve	Modifica	015473603-4	1	1301 7.0
BGGX	2014	07/05/2014 13:01:29	MTELLO	PERMISO18	Datos del Ve	Modifica	015473603-4	1	1301 7.0
GKWI	2014	07/05/2014 12:59:03	VROJAS	VICTORIAR(	Permisos de I	Agrega	013836993-5	4238 10	Permiso con Factura 1301 7.0
GKWI	2014	07/05/2014 12:58:59	VROJAS	VICTORIAR(	Datos del Ve	Modifica	013836993-5	10	1301 7.0
GKWI	2014	07/05/2014 12:58:56	VROJAS	VICTORIAR(	Permisos de I	Agrega	011528282-4	4238 10	Permiso con Factura 1301 7.0

14. PROCEDIMIENTOS DE CONTROL UTILIZADOS PARA EL ACCESO A LA RED, AL SISTEMA Y A LAS APLICACIONES

1.- Objetivo

Describir las políticas de control de acceso a los sistemas de información, acceso al dominio local y aplicaciones existente en la Municipalidad de San Joaquín.

Identificar los requerimientos de seguridad de cada una de las aplicaciones, como asi identificar toda la información relacionada con las aplicaciones y definir los perfiles de acceso de usuarios al dominio de la red en sus estaciones de trabajo.

2.- Alcance

Esta política se aplica a todos los funcionarios, funcionarios a contrata y a honorarios que tengan derechos de acceso a la información y que puedan afectar la información de la Municipalidad de San Joaquín que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información. Esta política se divulgara y será accesible a todos los funcionarios municipales.

3.- Reglas para el control de acceso a los sistemas & red local

Las reglas para el control de acceso, quedará estipulado bajo definidos por el departamento de Informatica, queda sujeto a la aplicación de una norma de calidad y cumplimiento un dictamen ó normativa legal.

3.1.- Política de utilización de los servicios de red

Se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

- Controlar el acceso a los servicios de red tanto internos como externos.
- Identificar las redes y servicios de red a los cuales se permite el acceso.
- Realizar normas y procedimientos de autorización de acceso entre redes.

- Establecer controles y procedimientos de administración para proteger el acceso y servicios de red

3.2.- Identificación de equipos en la Red

La Unidad de Informática controlará e identificará los equipos conectados a su red, mediante el uso de controladores de dominio, asignando una dirección IP, a cada usuario que se encuentre registrado en la red y dominio de SANJOAQUIN.

3.3.- Control de Acceso al Sistema Operativo

El acceso a los sistemas operativos estará protegido, mediante un inicio seguro de sesión, que contemplará las siguientes condiciones:

No mostrar información del sistema, hasta que el proceso de inicio se haya completado.

- No suministrar mensajes de ayuda, durante el proceso de autenticación.
- Validar los datos de acceso, una vez que se han diligenciado todos los datos de entrada.
- Limitar el número de intentos fallidos de conexión auditando los intentos no exitosos.
- No mostrar las contraseñas digitadas.
- No transmitir la contraseña en texto claro

3.3.- Gestión de contraseña

La asignación de contraseñas se deberá controlar a través de un proceso formal de gestión a cargo del Área de soporte y soporte de Sistemas. Las recomendaciones son:

No escribirlas en papeles de fácil acceso, ni en archivos sin cifrar.

- No habilitar la opción —recordar clave en este equipo", que ofrecen los programas
- Nunca guarde sus contraseñas, en ningún tipo de papel, agenda, etc.
- Las contraseñas se deben mantener confidenciales en todo momento.
- No compartir las contraseñas, con otros usuarios.
- Cambiar su contraseña si piensas que alguien más la conoce y si ha tratado de dar mal uso de ella.
- Selecciona contraseñas que no sean fáciles de adivinar.

- Nunca grabes tu contraseña en una tecla de función o en un comando de caracteres pre-definido.
- Cambia tus contraseñas regularmente.
- No utilizar la opción de almacenar contraseñas en Internet.
- No utilizar contraseña con números telefónicos, nombre de familia etc.
- No utilizar contraseña con variables

4.- Control de Acceso al Sistema Operativo

4.1.- Uso de utilitarios del sistema

Después de cinco (5) minutos de inactividad del sistema de Caschile, se considerará tiempo muerto y se bloqueará la sesión, sin cerrar las sesiones.

Los usuarios procederán a bloquear sus sesiones, cuando deban abandonar temporalmente su puesto de trabajo. Las estaciones de trabajo deberán quedar apagadas al finalizar la jornada laboral o cuando una ausencia temporal supere dos (2) horas.

4.2.- Limitación de tiempo de conexión Internet

El departamento de Informatica no limitará el tiempo de conexión, ni se establecerán restricciones en la jornada laboral.

4.3.- Control de acceso a la información

El control de acceso a la información a través de una aplicación, se realizará a través de roles que administren los privilegios de los usuarios dentro del sistema de información.

El control de acceso a información física o digital, se realizará teniendo en cuenta los niveles de clasificación y el manejo de intercambio de información definidos para el acceso a los recurso compartidos por cada dirección, según las reglas definidas para el acceso a las carpetas compartidas, estas son GLControl, GLDideco, GLGestionAdministratva, etc., quedando restringido el acceso por el servidor de dominios Active Directory, sujeto a los perfiles de acceso solicitados por los encargados de cada departamento ó dirección.

Para el acceso a internet por la UTM Perimetral de nuestro Firewall para los perfiles de usuarios; Firewall Usuario Full, Firewall Usuario Medio, Firewall Usuario Restringido restringido el acceso por los filtros de contenidos en Firewall perimetral.

ALEJANDRO ADIO QUINTUL
TECNICO INFORMATICO

YASNA ALBARRAN SOTO
DIRECTORA DE GESTION ADMINISTRATIVA