PROVINCIA DE SAN JUAN

CONSEJO FEDERAL DE INVERSIONES

ASESORAMIENTO Y CAPACITACIÓN
DIRECCIÓN PROVINCIAL DE INFORMÁTICA

INFORME FINAL

ABRIL 2011

PROF. PATRICIO ZUNINI

Índice

COMPENDIO

El objetivo del presente informe es realizar una descripción de las actividades que se han desarrollado durante el último año en la Dirección Provincial de Informática y el estado de los diferentes proyectos que se están encarando hacia el futuro acompañando lo definido en el marco del Plan Estratégico de la Secretaría de la Gestión Pública de la cual depende.

En primer lugar se presenta una descripción de las actividades relacionadas con el proyecto de elaboración de un reglamento interno de funcionamiento de las instalaciones del Centro Cívico en general y del equipamiento informático en el ámbito del gobierno en particular.

Asimismo, se han encarado distintos proyectos de desarrollo y rediseño de aplicaciones existentes que lleva adelante el Departamento de Sistemas de la Dirección Provincial de Informática, los que se describen en el presente. Entre ellos se desatacan el desarrollo de una aplicación para vincular los sistemas de Liquidación de Haberes con Presupuestos, la adaptación de la liquidación de haberes para el cálculo y pago de las asignaciones familiares y la personalización de un sistema de Mesa de Entradas.

Se realiza también una mención a las tareas que se están llevando adelante en relación a las necesidades de mantenimiento y actualización de la página web de la provincia.

Por otra parte, se presentan las actividades que viene desarrollando la Dirección Provincial de Informática en materia de capacitación para acompañar el desarrollo tecnológico de la provincia de San Juan. Esta capacitación procura realizar una actualización de los conocimientos conforme a las nuevas herramientas que se incorporan a la gestión y a las técnicas existentes.

Se describen, además, las tareas que se han encarado tendientes a la implantación de dos soluciones informáticas integrales. Es decir, que la aplicación de las soluciones no se remite exclusivamente al ámbito de la Dirección de Informática, sino que se procura que sean de utilización general en todo el ámbito del gobierno sanjuanino. Esto implica un verdadero desafío en la gestión de los

recursos y es posible gracias a la actuación de la Coordinación de Gobierno Electrónico.

En primer término se considera la incorporación de un servicio de directorio que permita mantener información actualizada sobre el stock de recursos informáticos, aplicaciones existentes y usuarios habilitados. Luego, se menciona la implantación de una solución integral de antivirus para el equipamiento de todas las dependencias del gobierno. Y finalmente se describen los proyectos de servicio de correo electrónico y hosting de sitios provinciales que está desarrollando la Dirección de Informática.

UTILIZACION DE EQUIPAMIENTO INFORMATICO – REGLAMENTO INTERNO

Antecedentes:

La evolución de la informática y los sistemas en la Administración Pública sanjuanina no escapa a las generales de la materia. Con la irrupción del procesamiento y la computación aparece en la provincia el primer equipamiento y con él, el 21 de agosto de 1969 mediante el decreto-acuerdo 129, se crea el primer centro de cómputos bajo la denominación de Centro de Sistematización de Datos. Dependiente del Ministerio de Economía su finalidad era ser "*el órgano ineludible de ejecución, asesoramiento y consulta de todo proceso que pueda ser cumplido por los medios técnicos, mecánicos o electrónicos con que se contare".* Simultáneamente se procede a la contratación del alquiler de la computadora electrónica IBM 360/20 y equipo complementario.

El 1 de noviembre de 1982, mediante el decreto 2022, el gobernador de la provincia aprueba el Organigrama Jerárquico y el Manual de Misiones y Funciones. Posteriormente, mediante el decreto 1253 del 21 de julio de 2000, se decide el cambio de denominación por el de Dirección Provincial de Informática y, mediante el decreto 1254, se establece que *"los Organismos Centralizados y Descentralizados, dependientes del Poder Ejecutivo Provincial, deberán solicitar la intervención y opinión de la DIRECCION PROVINCIAL DE INFORMATICA, suministrando toda la información relativa a sus proyectos de adquisición o arrendamientos de bienes y servicios de carácter informático y sus comunicaciones asociadas, antes de proceder a la respectiva convocatoria para presentar ofertas y con una antelación que permita su adecuada evaluación".*

Posteriormente la aparición de las computadoras personales comenzó a producir un proceso de descentralización del procesamiento de la información favorecido por la circunstancia de la reducción en los costos y de la existencia de numerosas reparticiones localizadas en distintos edificios. Esto acompañado por el surgimiento de internet que facilitaba las comunicaciones y la transferencia de información.

A raíz de la inauguración del Centro Cívico, edificio que centraliza la localización de la mayoría de las reparticiones de la Administración Pública

Sanjuanina, surge la necesidad de comenzar a coordinar diferentes tareas que se realizaban en forma descentralizada.

Con este objetivo, entre otros, es que se conformó la Coordinación de Gobierno electrónico mediante decreto acuerdo de ministros. La misma depende de la Secretaría de la Gestión Pública y está conformada por cinco subcoordinaciones o grupos:

- Data Center: se encarga de la administración y utilización del espacio reservado para el resguardo de los servidores. Está a cargo del Lic. Gustavo Quiroga, responsable del Área de Sistemas del Ministerio de Educación.
- Sistemas y Bases de Datos: tiene la responsabilidad de coordinar los desarrollos de sistemas y la interoperabilidad de las bases de datos que se generen. La idea principal es que no se realicen desarrollos redundantes de aplicaciones y que la infraestructura de datos que administra la provincia sea consistente. Esta subcoordinación está a cargo del Lic. Gustavo Sacks, Director Provincial de Informática.
- Telecomunicaciones: el objetivo de ésta es coordinar la interconexión de las distintas redes informáticas y la administración de las mismas, de modo que se potencien los emprendimientos y se ahorren esfuerzos. La misma está bajo la responsabilidad del Ing. Carlos Larisson, Subsecretario de Telecomunicaciones y Proyectos Especiales.
- Servicios TI: se trata de administrar los servicios de Tecnología de la Información que utiliza la provincia y de gerenciar los proyectos que para tales efectos se encaren como ser correo electrónico, antivirus, etc. Esta área se encuentra bajo la supervisión del Lic. Horacio Sánchez, profesional contratado de la Dirección Provincial de Informática.
- Sitio Web: Administra el sitio web provincial y los servicios que dependen del mismo como la guía de trámites. Está a cargo del Sr.

Ramón Roqueiro, quien a su vez es el Coordinador de Gobierno Electrónico.

En este ámbito se planteó la necesidad de establecer políticas y pautas para la utilización del equipamiento informático en el Centro Cívico y que posteriormente sean extensivas a toda la Administración Pública Provincial. Estas pautas están incluidas en un reglamento general desarrollado por la Secretaría de la Gestión Pública junto con la Dirección de Control Operativo del Centro Cívico. El mismo se encuentra para la aprobación. Dicho reglamento se incluye como anexo I en el presente informe.

En materia informática, en líneas generales se analizaron pautas para los siguientes ejes temáticos:

- Hardware: se deberá controlar y autorizar el equipamiento que se instale de manera que cumpla con los estándares establecidos por la Dirección Provincial de Informática. La instalación de servidores deberá realizarse exclusivamente en el espacio reservado para los mismos en el Data Center.
- Software: en este aspecto se hace necesario dejar claramente establecido que el software instalado en los equipos deberá contar con la correspondiente licencia de uso o tratarse de software de libre licenciamiento, quedando bajo responsabilidad del usuario del equipo y del responsable de la repartición la utilización indebida del mismo.
- Servicio de Internet y correo electrónico: se hace constar que el servicio de Internet se otorga con la finalidad que el mismo sea usado exclusivamente para la gestión y tareas que demande la Administración Pública y que las conexiones inapropiadas a Internet pueden dar lugar a que usuarios no autorizados obtengan acceso a las redes internas. Por otra parte, los usuarios autorizados deben utilizar como medio de comunicación el software y el hardware de salida

provisto por el Gobierno. Asimismo, no está permitido realizar la descarga de programas, música, videos ni ninguna otra aplicación que infrinja la ley de propiedad intelectual y está prohibido transmitir por Internet información confidencial, material que viole derechos de autor, material obsceno o información protegida por secreto comercial. Finalmente se estableció como página de inicio de la sesión del navegador la correspondiente al Sitio Oficial del Gobierno de San Juan, cuya dirección es www.sanjuan.gov.ar

- Confidencialidad de la Información: en este aspecto se hace referencia a que no está permitido utilizar el logotipo y nombre del Gobierno Provincial, sistemas, bases de datos, informaciones internas, informes gerenciales, y otras similares en servidores de acceso público o de terceros sin la correspondiente aprobación del responsable de la Repartición correspondiente. Además, está prohibida la utilización de información en cualquier formato o estructura fuera del ámbito laboral y distinta a la finalidad para la cual fuera conformada sin la correspondiente autorización.

Con respecto al tema de la confidencialidad de los datos, se reiteró firmemente la necesidad de conocer y cumplir la ley de Hábeas Data, para lo cual se realizó una serie de charlas para el personal responsable de administrar bases de datos de la Dirección Provincial de Informática. En el anexo II se incluye la mencionada ley.

Uno de los temas que más preocupación ha generado en la Coordinación de Gobierno electrónico es el diseño, acceso y utilización del espacio diseñado en el Centro Cívico como Data Center. El Data Center es el espacio común y compartido donde residen los servidores de todas las reparticiones y se encuentra en el subsuelo del edificio. Ante la incorporación de gran cantidad de servidores por parte de las distintas reparticiones, ha aumentado considerablemente la demanda de espacio en el Data Center y resulta necesario realizar una adecuación de las instalaciones para optimizar la utilización del mismo. Además, se está haciendo un análisis del estado del mismo para evaluar en qué grado cumple con los estándares

internacionales y realizar las mejoras necesarias para adecuarlo a lo óptimo. En este sentido, el responsable Lic. Gustavo Quiroga está llevando adelante las gestiones necesarias para acondicionarlo y establecer las pautas de acceso sugeridas en el estándar TIA-942 que se desarrollan a continuación.

El estándar TIA-942

Un estándar es un compendio de buenas prácticas que son aceptadas por consenso, y que eventualmente pueden constituirse en una normatividad con fuerza de Ley en algunos países. El estándar da unos lineamientos aceptados por consenso en el marco de instituciones o agremiaciones que investigan dichas buenas prácticas.

Así la TIA (Telecommunications Industry Association), publicó en Abril de 2005, el estándar de telecomunicaciones para Centros de Datos con la intención de unificar criterios en el diseño de áreas de tecnología y comunicaciones. Este estándar que en sus orígenes se basa en una serie de especificaciones para comunicaciones y cableado estructurado, avanza sobre los subsistemas de infraestructura generando los lineamientos que se deben seguir para clasificar estos subsistemas en función de los distintos grados de disponibilidad que se pretende alcanzar.

Basado en recomendaciones del Uptime Institute, establece cuatro niveles (tiers) en función de la redundancia necesaria para alcanzar niveles de disponibilidad de hasta el 99.995%.

A su vez divide la infraestructura soporte de un datacenter en cuatro subsistemas a saber:

- Telecomunicaciones
- Arquitectura
- Sistema eléctrico
- Sistema Mecánico

1 Consideraciones arquitectónicas.

2 accesos al edificio desde rutas\calles separadas.

Preferentemente edificio de una planta dedicado exclusivamente a datacenter

Otros usuarios del edificio si los hay no deberán dedicarse a actividades industriales.

La posible altura de la sala del centro de datos debe tenerse en cuenta, ya que alturas de 4 metros pueden ser necesarias para albergar la totalidad de la instalación.

Existencia de un muelle de descarga.

Distancia a fuentes de radiaciones electromagnéticas y de radiofrecuencia.

Ubicación por encima de los niveles de agua. Nunca deben instalarse sistemas críticos en los sótanos.

No ubicar la sala de alojamiento bajo salas con instalaciones de cañería de agua.

La sala no debe tener ventanas.

2. Consideraciones eléctricas

Un CPD es un caso típico de una instalación donde, debido a la extrema importancia de la información allí contenida y a la continuidad de los servicios que se le exige, la energía suministrada debe estar siempre disponible. Debido a esta importancia, a estos equipos se les suele llamar “equipos críticos”, haciendo alusión a que su mal funcionamiento, o desperfecto, sería “crítico” para los intereses de una empresa u organismo.

Por supuesto que la importancia de estos equipos críticos es relativa al servicio que brindan. Un desperfecto momentáneo puede ocasionar una pérdida de competitividad (como en el caso que una terminal de venta al público de boletos de avión de una determinada empresa no pueda acceder al CPD para saber el saldo de los boletos para un determinado vuelo), o puede ocasionar una pérdida importante

de ingresos a la empresa (como sería el caso que el CPD de una tarjeta de crédito internacional no respondiera a las solicitudes de crédito durante 1 hora), o hasta la total desaparición de la misma (como sería el caso que el CPD de un banco pierda los datos de sus depósitos).

Debido a esta criticidad es que desde hace años se estudian distintas topologías, o formas de realizar la instalación eléctrica en estos sitios, de forma que las fallas y mal funcionamientos comunes no afecten el servicio del CPD. En otras palabras, se han analizado las fallas comunes en una instalación eléctrica (cortocircuitos, cortes de energía desde la red, la falla o demora de encendido de un grupo electrógeno, la falla de un interruptor termomagnético, etc.) así como las tareas habituales que deben hacerse sobre la misma (ampliar un tablero de distribución, agregar un interruptor en un tablero general, sustitución de una línea de potencia, sustitución de un interruptor, etc.) y cómo evitar que estas tareas afecten el servicio de los equipos críticos (CPD).

Una forma convencional de análisis ha sido considerar el tiempo medio entre fallas (MTBF) así como el tiempo medio de reparación (MTTR) de los distintos elementos que integran una instalación eléctrica, y estimar el MTBF y el MTTR de toda la instalación. Esto ha llevado a distintas formas y teorías de análisis. Sin embargo, la mayoría de las mismas adolecen de no poder considerar los errores humanos, o por suponer situaciones ideales de trabajo (que siempre tengamos el repuesto necesario al alcance nuestro, que la instalación de los equipos es la adecuada, etc.) cosa que el que hace mantenimiento sabe que la mayoría de las veces no se cumplen.

Verificar la capacidad de las acometidas eléctricas al edificio, disponibilidad de más de un proveedor y/o subestaciones eléctricas distintas y que el edificio dispone de acometidas eléctricas subterráneas.

3. Telecomunicaciones

El edificio debe disponer de al menos 2 entrance rooms de fibra óptica que sigan caminos diferentes.

Estas acometidas de fibra deben terminar en ubicaciones físicas distintas de los proveedores.

Diversos proveedores de servicios de telecomunicaciones tienen que ofrecer servicios en las instalaciones.

El equipamiento de telecomunicaciones debe estar instalado en el área del datacenter y no en áreas compartidas del edificio. El cableado debe estar adecuadamente canalizado, estar dedicado a telecomunicaciones y no ser accesible a terceros.

4. Seguridad

Accesibilidad 24 x 7 x 365.

Monitorización de accesos, parking y muelle de descarga y resto de zonas comunes.

El edificio no deberá ubicarse en una zona con riesgo medio de inundaciones o superior, es decir frecuencia inferior a 100 años y calado alto (0,8 m), o en áreas con riesgos sísmicos, o de otro tipo de catástrofes.

No se ubicará el CPD en edificios que puedan resultar dañados por edificios colindantes durante un terremoto o inundación.

El edificio no podrá ubicarse en los pasillos aéreos de aeropuertos.

El edificio se ubicará como mínimo a 0,4 Km. de aeropuertos, ríos, la costa o presas con reservas de agua.

El edificio debe ubicarse a menos de 0,8 Km de autopistas.

El edificio estará como mínimo a 0,8 Km. de bases militares.

El edificio no se ubicará a menos de 1,6 Km. de centrales nucleares, polvorines y fábricas de armamento.

El edificio no se ubicará adyacente a una embajada extranjera.

Se indicará la proximidad de estaciones de policía, parque de bomberos y hospitales.

Entendiendo los tiers.

Uno de los mayores puntos de confusión en el campo del uptime (tiempo disponible de los sistemas) es la definición de datacenter confiable; ya que lo que es aceptable para una persona o compañía no lo es para otra. Empresas competitivas con infraestructuras de datacenter completamente diferentes proclaman poseer alta disponibilidad; esto puede ser cierto y dependerá de la interpretación subjetiva de disponibilidad que se realice para el tipo de negocio en que se encuentre una compañía.

Lo cierto es que para aumentar la redundancia y los niveles de confiabilidad, los puntos únicos de falla deben ser eliminados tanto en el datacenter como en la infraestructura que le da soporte.

Los cuatro niveles de tiers que plantea el estándar se corresponden con cuatro niveles de disponibilidad, teniendo que a mayor número de tier mayor disponibilidad, lo que implica también mayores costos constructivos.

Esta clasificación es aplicable en forma independiente a cada subsistema de la infraestructura (telecomunicaciones, arquitectura, eléctrica y mecánica). Hay que tener en cuenta que la clasificación global del datacenter será igual a la de aquel subsistema que tenga el menor número de tier. Esto significa que si un datacenter tiene todos los subsistemas tier IV excepto el eléctrico que es tier III, la clasificación global será tier III.

Es importante tener en cuenta esto porque cuando se pretende la adecuación de datacenters actuales a tier IV, en lugares como América Latina, hay limitaciones físicas difíciles de salvar en los emplazamientos edilicios actuales. Prácticamente para lograr un datacenter tier IV hay que diseñarlos de cero con el estándar en mente como guía. Un ejemplo claro de esto es que es muy difícil lograr la provisión de energía de dos subestaciones independientes o poder lograr las alturas que requiere el estándar en los edificios existentes (3 m mínimo sobre piso elevado y no menor de 60 cm entre el techo y el equipo más alto).

La norma describe, resumidamente, los distintos tiers de la manera que sigue:

Tier I: datacenter básico

Un datacenter tier I puede ser susceptible a interrupciones tanto planeadas como no planeadas. Cuenta con sistemas de aire acondicionado y distribución de energía; pero puede o no tener piso técnico, UPS o generador eléctrico; si los posee pueden no tener redundancia y existir varios puntos únicos de falla. La carga máxima de los sistemas en situaciones críticas es del 100%. La infraestructura del datacenter deberá estar fuera de servicio al menos una vez al año por razones de mantenimiento y/o reparaciones. Situaciones de urgencia pueden motivar paradas más frecuentes y errores de operación o fallas en los componentes de su infraestructura causarán la detención del datacenter. La tasa de disponibilidad máxima del datacenter es 99.671% del tiempo. El tiempo de parada del CPD a lo largo de un año es de 29 horas como máximo.

Tier II: componentes redundantes

Los datacenters con componentes redundantes son ligeramente menos susceptibles a interrupciones, tanto planeadas como las no planeadas. Estos datacenters cuentan con piso falso, UPS y generadores eléctricos, pero están conectados a una sola línea de distribución eléctrica. Su diseño es “lo necesario más uno” (N+1), lo que significa que existe al menos un duplicado de cada componente de la infraestructura. La carga máxima de los sistemas en situaciones críticas es del 100%. El mantenimiento en la línea de distribución eléctrica o en otros componentes de la infraestructura puede causar una interrupción del procesamiento.

La tasa de disponibilidad máxima del datacenter es 99.749% del tiempo. El tiempo de parada del CPD a lo largo de un año a 22 horas como máximo.

Tier III: mantenimiento concurrente

Las capacidades de un datacenter de este tipo le permiten realizar cualquier actividad planeada sobre cualquier componente de la infraestructura sin interrupciones en la operación. Actividades planeadas incluyen mantenimiento

preventivo y programado, reparaciones o reemplazo de componentes, agregar o eliminar elementos y realizar pruebas de componentes o sistemas, entre otros. Para infraestructuras que utilizan sistemas de enfriamiento por agua significa doble conjunto de tuberías. Debe existir suficiente capacidad y doble línea de distribución de los componentes, de forma tal que sea posible realizar mantenimiento o pruebas en una línea, mientras que la otra atiende la totalidad de la carga. En este tier, actividades no planeadas como errores de operación o fallas espontáneas en la infraestructura pueden todavía causar una interrupción del datacenter. La carga máxima en los sistemas en situaciones críticas es de 90%. Muchos datacenters tier III son diseñados para poder actualizarse a tier IV, cuando los requerimientos del negocio justifiquen el costo. La tasa de disponibilidad máxima del datacenter es 99.982% del tiempo. El tiempo de parada del CPD a lo largo de un año a 1,5 horas como máximo.

Tier IV: tolerante a fallas

Este datacenter provee capacidad para realizar cualquier actividad planeada sin interrupciones en las cargas críticas, pero además la funcionalidad tolerante a fallas le permite a la infraestructura continuar operando aun ante un evento crítico no planeado. Esto requiere dos líneas de distribución simultáneamente activas, típicamente en una configuración system + system; eléctricamente esto significa dos sistemas de UPS independientes, cada sistema con un nivel de redundancia N+1. La carga máxima de los sistemas en situaciones críticas es de 90% y persiste un nivel de exposición a fallas, por el inicio una alarma de incendio o porque una persona inicie un procedimiento de apagado de emergencia o Emergency Power Off (EPO), los cuales deben existir para cumplir con los códigos de seguridad contra incendios o eléctricos. La tasa de disponibilidad máxima del datacenter es 99.995% del tiempo. El tiempo de parada del CPD a lo largo de un año a 26 minutos como máximo.

En definitiva, el propósito del estándar TIA 942 es proveer una serie de recomendaciones y guidelines para el diseño e instalación de un datacenter. La intención es que sea utilizado por los diseñadores que necesitan un conocimiento acabado del facility planning, el sistema de cableado y el diseño de redes.

El estándar TIA 942 y la categorización de tiers se encuentran en pleno auge en América Latina. Esto es bueno porque lleva al replanteo de las necesidades de infraestructura de una manera racional y alineada con las necesidades propias de disponibilidad del negocio en que se encuentran las organizaciones.

REDISEÑO Y DESARROLLO DE SISTEMAS

Generalidades

Dentro de la estructura interna de la Dirección Provincial de Informática se encuentra el departamento de Sistemas que es el responsable del desarrollo y mantenimiento de distintas aplicaciones de la Administración Pública Provincial.

Esta área está compuesta por un jefe de departamento, un responsable de la división Análisis y otro de la división Programación.

La división análisis cuenta con cuatro analistas y la división programación con doce programadores. Este plantel se encuentra en este momento en un proceso de actualización de sus conocimientos acorde a las nuevas tendencias que impone la tecnología informática. En este sentido ya se han realizado cursos sobre programación php, programación C# y actualmente se está realizando capacitación sobre programación ASP.

El objetivo buscado es adecuar los conocimientos para poder encarar con tecnologías actualizadas los nuevos desarrollos. Actualmente el área de Sistemas de la DPI está realizando los proyectos que a continuación se describen:

1. Vinculación de los haberes con el presupuesto:

Uno de los desafíos propuestos por la Secretaría de la Gestión Pública y patrocinado por el Ministerio de Hacienda de la Provincia es lograr vincular la información de la liquidación con la de la Contabilidad Presupuestaria.

Actualmente existen dos aplicaciones que administran información complementaria:

- Sistema de Liquidación de Haberes
- Sistema de Administración Financiera (TRADFIN)

El sistema por el cual se liquidan los sueldos data de la década del 70, al cual se le introdujeron cambios para su adecuación a medida que las necesidades así lo requirieron o por la adquisición de nuevas tecnologías.

Básicamente consta de un archivo maestro (EBCDIC-Secuencial) con algunos parámetros de liquidación y datos personales del agente que se relaciona mediante el Escalafón o Régimen y la Categoría del agente con otro archivo (EBCDIC-Secuencial) que contiene las escalas de sueldos de todos los escalafones para el mes que se trate.

Este archivo maestro se actualiza con las novedades informadas por los liquidadores de cada repartición (SQL).

Las novedades son grabadas en forma local o remota en tablas SQL y actualizan el maestro en modo BATCH.

Sobre este maestro actualizado se realizan los distintos procesos para cargas la escala salarial y calcular conceptos remunerativos, aportes y contribuciones, cuotas gremiales, cuotas de seguro de vida de La Caja, etc.

Se obtiene axial un archivo de similar estructura al de entrada pero con los parámetros transformados en conceptos a pagar y a descontar.

A partir de este (Archivo liquidado) se generan las distintas salidas impresas o en soporte magnético.

Una de esas salidas son reportes para informar al Sistema TRADFIN.

El problema principal radica en que los dos sistemas se han concebido y desarrollado en forma autónoma lo que ha generado que las tablas y archivos que almacenan los datos no se correspondan en forma unívoca. Por otra parte la información presupuestaria posee una apertura que no se condice con los datos almacenados para la liquidación de haberes.

Para poder realizar la interoperabilidad entre los dos sistemas se está desarrollando una aplicación que permita determinar sobre los agentes liquidados a qué unidad de la estructura programática pertenecen, de manera de poder relacionar cada unidad con una cuenta del presupuesto y poder imputar mensualmente el gasto en personal conforme a la información requerida.

En estos momentos se están relevando los datos del personal y se están desarrollando un módulo de carga para que el área contable informe las cuentas correspondientes a cada unidad organizativa.

2. Adaptación del Sistema de Liquidación de Haberes:

Con la liquidación del mes de agosto de 2010 se puso en práctica la nueva modalidad de pago de asignaciones familiares para empleados de la administración pública determinada por ley provincial. Esta nueva modalidad se asemeja a la ley nacional aunque con montos menores y conservando, en algunos casos, los montos de la modalidad anterior en forma de pago residual para evitar que haya agentes que dejen de cobrar. Por otra parte, si bien existen distintos tramos según los cuales varían los importes de los conceptos, no existe tope, es decir, todos los empleados de la administración pública provincial que tengan alguna carga de familia percibirán un importe determinado.

Para poder cumplir con esta ley de reciente sanción se debieron llevar a cabo tareas de análisis y programación que pudieron terminarse a término para realizar la liquidación.

Hasta el momento los controles efectuados no evidencian inconvenientes en el proceso.

En estos momentos se está encarando el desarrollo de una aplicación complementaria que permita administrar la información del grupo familiar de los empleados de manera de poder tener registrados los datos de los individuos que generan la asignación familiar que se abona. Se prevé que esta información sea validada con la de la Obra Social para poder tener mayor consistencia.

3. Sistema de Seguimiento de Expedientes:

En la actualidad, las distintas reparticiones de la Administración Pública de la provincia realizan el registro y seguimiento interno de los expedientes de manera autónoma, siendo en muchos casos de forma manual y en otros con aplicaciones sencillas que no poseen una funcionalidad completa.

La idea que se promueve actualmente desde la Secretaría de la Gestión Pública es la de la implantación de un sistema único de gestión de expedientes que permita unificar el registro y seguimiento en una sola plataforma.

En este sentido se han analizado distintas alternativas. Inicialmente se implantó a modo de prueba el Sistema de Mesa de Entradas del Ministerio de Defensa de la Nación que fue cedido mediante la firma de un convenio. Para ello, se instaló la aplicación en un servidor de la Dirección Provincial de Informática y comenzó a utilizarse a modo de prueba en las reparticiones dependientes de la Secretaría de la Gestión Pública. Se realizó la capacitación de personal técnico, se crearon los usuarios autorizados para operarlo, se definieron los distintos tipos de trámites y las estructuras correspondientes. Se realizó la prueba correspondiente pero no resultó totalmente satisfactoria, por lo cual se decidió realizar el análisis y prueba del sistema COMDOC II, cedido oportunamente por el Ministerio de Economía de la Nación. Esta aplicación resultó mucho más amigable y actualmente se encuentra en producción para las reparticiones dependientes de la Secretaría de la Gestión Pública de la Provincia. Una vez estabilizado el sistema se estima ampliar el mismo a otras áreas.

REDISEÑO DEL SITIO WEB

Una de las aplicaciones desarrolladas bajo tecnología web en el ámbito del Ministerio de Hacienda y Finanzas es el Sitio Web de la Dirección General de Rentas.

Según la información brindada por Departamento de Programación y Planificación Estratégica de la Dirección General de Rentas, el sitio actualmente opera en un servidor que pone a disposición de los contribuyentes el servicio Web Público y que también realiza las operaciones de análisis de las DDJJ presentadas, su grabación y posterior emisión de comprobantes correspondientes. Este servidor interactúa con los otros dos servidores que contienen las bases de datos actuales de Oracle y Sybase.

Si bien desde la implementación de presentaciones de Declaraciones Juradas en WEB desde Setiembre de 2009, se efectuaron diversas correcciones de mejora en el diseño de administración del sitio WEB, estas mejoras no han podido superar la enorme demanda de presentaciones, a la vez que se incremento significativamente el uso de la página para la prestación de servicios de los contribuyentes.

El volumen de operaciones por mes actualmente es de alrededor de 21.000 operaciones, de las cuales el 76 % lo realizan usuarios con clave de Usuario Registrado (alrededor de 16.400 operaciones), y de este último valor las DDJJ representan el 87% de las operaciones (alrededor de 14.200).

La operación de la registración de una DDJJ es el proceso más costoso en términos de uso de recursos de los servidores.

Los pasos actuales para el proceso de cada Declaración Jurada de contribuyentes de Ingresos Brutos son:

1. El contribuyente sube el archivo comprimido de la DDJJ a la página web.
2. El servidor web (donde se aloja la página web), procede a depositar el archivo recibido en una carpeta.
3. Un aplicativo procede a descomprimir este archivo y el contenido del mismo (4 archivos: cabecera de DDJJ con totales, detalle de DDJJ con datos de bases imponibles, retenciones/percepciones de DDJJ con los datos de los

certificados y pagos DDJJ con datos de pagos a cuenta en caso de rectificativas), se deposita en tablas temporales para su selección y posterior análisis y cálculo de los datos presentados.

4. Se envía una grilla de datos de las presentaciones contenidas en el archivo para que el contribuyente realice la elección.

5. Luego de seleccionada la declaración correspondiente, se procede al análisis y cálculo de los datos descomprimidos.

6. Se envían estos datos a una página web de confirmación de la Declaración Jurada, previo paso a la impresión del acuse y/ boleta de pago.

7. Finalmente, luego de la confirmación, se procede a la grabación en las tablas correspondientes: DDJJ, cuenta corriente y vencimientos (en el caso que haya importe a pagar) del contribuyente.

8. El aplicativo le pasa los datos de la constancia de recepción y la boleta de pago (cuando correspondiere) al otro aplicativo que realiza la impresión del mismo en una impresora virtual Adobe Acrobat, generando el archivo PDF correspondiente.

9. Finalmente el aplicativo anterior le devuelve a la página web el archivo para su visualización e impresión.

Todos estos pasos son ejecutados actualmente por un solo servidor.

Debilidades del Diseño Actual:

- Un único Servidor afectado a operaciones WEB en la que se producen las tareas de subida de archivos, descompresión, grabación temporal del archivo DDJJ y procesamiento en las tablas de registración del Sistema de la DGR.
- Esto produce cuellos de botella en los procesos. Conforme a la estadística actual se produjo un máximo de presentaciones de 150 a 160 DDJJ por hora en sus picos máximos.
- Actualmente se producen registraciones máximas de DDJJ equivalentes a 2.000 en forma diaria.

- Se observa que el 50% de los usuarios presentan sus DDJJ antes del comienzo de los vencimientos, pero el límite máximo de presentaciones a procesar es muy ajustado para el remanente de DDJJ (el otro 50%).
- La tendencia es creciente mes a mes de cantidad de presentaciones. Se estima que la incorporación de Agentes de Percepción producirá un aumento equivalente al 8% más de DDJJ para el mes de Agosto.
- No disponemos una cobertura óptima de mesa de asistencia al usuario y limitada en sus horarios de prestación, con teléfono a cuenta del usuario.

Meta Propuesta:

- Lograr un umbral máximo de procesamiento diario de 4.000 DDJJ
- Reducción máxima de la cola de procesamientos en registración Batch (offline)
- Descentralización de la recepción de DDJJ en diferentes servidores, lo que disminuye los tiempos de procesamiento y optimizara el servicio de las aplicaciones WEB de la página.

Para lograr el objetivo se ha elaborado un proyecto que se puso a consideración de las autoridades del Ministerio de Hacienda y fue considerado satisfactorio, con lo cual se ha dado comienzo al mismo. Inicialmente se ha adquirido equipamiento de última tecnología lo que permite mejorar los tiempos de procesamiento y eliminar los cuellos de botella que se puedan producir. Actualmente se está llevando adelante la configuración del equipamiento y la puesta a punto del mismo.

CAPACITACIÓN INFORMÁTICA

Uno de los objetivos perseguidos por la Dirección Provincial de Informática es el de adecuar el perfil de sus recursos humanos a las aplicaciones y herramientas existentes en la actualidad y a los desafíos que las tecnologías de la información y comunicaciones plantean hacia el futuro.

En este sentido, se ha encarado un programa de capacitación que apunta a fortalecer las técnicas de programación y consolidar los aspectos de seguridad informática que se encontraban retrasados conforme las necesidades actuales.

Como parte de esta capacitación se han encarado a lo largo de este año actividades que involucraron a empleados de distintos departamentos de la Dirección Provincial de Informática:

Departamento de Sistemas

Uno de los principales destinatarios de la capacitación encarada es el personal que cumple tareas en el departamento de Sistemas. Ellos son los responsables del desarrollo y mantenimiento de aplicaciones informáticas para la administración pública provincial. Por ello se destinaron 120 (ciento veinte) horas de capacitación para llevar adelante dos cursos destinados a 10 (diez) programadores y analistas. El objetivo de los cursos era instruir al personal en la programación en el ambiente web.

Se elaboraron planes de capacitación que incluye framework, .NET y C#.

En el desarrollo de software, un *framework* es una estructura de soporte definida previamente, en la cual otro proyecto de software puede ser organizado y desarrollado. Típicamente, un *framework* puede incluir soporte de programas, bibliotecas y un lenguaje interpretado entre otros software para ayudar a desarrollar y unir los diferentes componentes de un proyecto.

Un framework representa una arquitectura de software que modela las relaciones generales de las entidades del dominio (bases de datos, objetos). Provee una estructura y una metodología de trabajo.

Los framework son diseñados con el intento de facilitar el desarrollo de software, permitiendo a los diseñadores y programadores pasar más tiempo identificando requerimientos de software que tratando con los detalles de bajo nivel de proveer un sistema funcional.

En otras palabras un framework representa una arquitectura de software que modela las relaciones generales, provee una estructura y una metodología de trabajo, con lo cual podemos decir que los framework son diseñados con la intención de facilitar en gran medida el desarrollo de software.

En el Anexo III se presenta una lista con los temas destacados de los cursos mencionados.

Departamento de Recursos

En el caso del departamento de Recursos, la capacitación encarada se basó en cubrir aspectos de seguridad informática que se consideró que debían ser reforzados.

En primer lugar, y acompañando el proceso de migración de las cuentas de correo electrónico del gobierno de San Juan, se procedió a capacitar al personal de este departamento en el uso de Microsoft Exchange. Exchange es un servidor de comunicación de la empresa Microsoft basado en el correo electrónico de colaboración empresarial.

Dado que el proyecto que actualmente lleva el Ministerio de Educación de la Provincia de San Juan incluye la implantación de la solución Exchange para el personal de dicho ministerio y que se resolvió aplicar esa solución para todo el ámbito de toda la administración pública, se procedió a la migración de las cuentas de correo que se encontraban alocadas en un servidor de un proveedor en Buenos Aires hacia otro que reside en el Data Center del Centro Cívico de San Juan. A raíz de esta migración se logró avanzar en la administración centralizada de las cuentas por parte del personal de la Dirección Provincial de Informática.

Este proceso trajo aparejada la correspondiente capacitación de un equipo de 10 (diez) personas que procedió a realizar las siguientes tareas:

- Relevamiento de las cuentas de correo existentes
- Depuración de las cuentas sin movimiento
- Notificación del proceso de migración a realizar
- Configuración del servidor de correo
- Migración de las cuentas
- Configuración de las cuentas Outlook en las computadoras personales
- Asistencia telefónica mediante una mesa de ayuda instalada a los efectos
- Elaboración del proceso de alta, baja y mantenimiento de las cuentas
- Mantenimiento de las cuentas

Actualmente se están analizando otras funcionalidades de la herramienta Exchange como ser el uso de agendas compartidas, espacio para compartir carpetas, etc. de manera de realizar posteriormente la capacitación del personal que implementará estas soluciones en las distintas reparticiones que así lo requieran.

Por otra parte se está trabajando con un grupo de empresas de la Cámara Sanjuanina de Empresas de Tecnologías de Informática y Comunicación (CASETIC) en la elaboración de un diagnóstico sobre materia de Seguridad Informática de las distintas áreas de la Dirección Provincial de Informática. El objetivo de este relevamiento es realizar un diagnóstico de la situación a fin de encarar un proceso de mejoras mediante capacitación y reformulación de procesos para el año próximo.

Además se realizó la capacitación de dos agentes en materia de Habeas Data para que dictaran un curso al resto de los empleados de la DPI. Esta cuestión resulta importante dado que existen limitaciones legales en la administración de los datos personales que se almacenan en las distintas bases de datos. Dado que la Dirección Provincial de Informática administra bases de datos con información personal resulta imprescindible que sus empleados conozcan lo que indican las leyes al respecto. En el Anexo II y IV se adjuntan la legislación provincial y nacional vigente en la materia.

SERVICIO DE DIRECTORIO

Generalidades:

La infraestructura tecnológica del Gobierno de San Juan en la actualidad se encuentra en un estadio inicial de desarrollo. Comienzan a plantearse problemáticas parecidas en diversos ámbitos. Distintas áreas de gobierno comienzan a desarrollar soluciones diferentes para requerimientos similares. La gestión de seguridad, la posibilidad de integración de las soluciones desplegadas, y la interoperabilidad son algunos de los objetivos principales de todo desarrollo tecnológico ordenado.

Las organizaciones modernas, se ven sometidas a una enorme dinámica en lo referente a crecimiento y actualización. Una de las prácticas aconsejables en el contexto antes definido es contar con sistemas, servicios e infraestructura básica debidamente diseñada e implementada. La adecuación a estándares se vuelve esencial. En este sentido se está trabajando desde la Coordinación de Gobierno Electrónico, cuyo principal objetivo es generar un ámbito de diálogo entre los referentes de las reparticiones que mayor demanda de tecnología generan, de manera de consensuar políticas, compartir recursos y ahorrar esfuerzo generando sinergia entre las distintas áreas.

El Servicio de Directorio (SD en adelante) es uno de los pilares básicos y transversales necesarios. Sobre el SD se construye el conjunto de servicios que conforma la Infraestructura TI de las organizaciones modernas.

Un SD es un conjunto de componentes que brindan el servicio, a nivel informático, de administración, almacenamiento y organización de la información sobre usuarios y recursos de una red de computadoras. Fundamentalmente facilita, a administradores, la gestión del acceso de usuarios/aplicaciones a los diversos recursos existentes en las redes. Esta gestión se lleva a cabo de manera centralizada y transversal a la infraestructura TI. Es decir, un SD implementa un repositorio central, adecuadamente organizado, para almacenar información de una red informática y recursos asociados. Y en especial define estándares de operabilidad dentro de la red. Una consideración clave, es que debidamente desplegada esta solución (SD) es posible la delegación de la administración en unidades menores, logrando así reflejar en cierta forma la realidad organizativa de Gobierno.

Los beneficios asociados son diversos, pero podemos citar los siguientes con el fin de comprender con más detalle la importancia de un SD:

Administración centralizada de la Infraestructura Tecnológica.

Capacidad de subdivisión y delegación de la administración.

Gestión y aplicación de políticas de seguridad a distintos niveles, con la suficiente granularidad para asegurar la Infraestructura tecnológica.

Definición de estándares y protocolos comunes.

Autentificación Única o en inglés “Single Sign-On”. Este procedimiento permite iniciar una sesión en una estación de trabajo y acceder a diversos servicios dentro de la red sin tener que volver a autentificarse. Estos servicios pueden ser: cuentas de correo electrónico o mensajería, recursos compartidos (impresoras y carpetas), conectividad (internet o redes privadas), aplicaciones, sistemas, accesos físicos a diversa áreas, entre otros.

Generación de reportes y auditorías para monitoreo del uso de los recursos computacionales.

Gestión de la identidad dentro de la red. Un SD es el soporte ideal para la distribución de œrtificados electrónicos personales, específicamente, un servicio de directorio resuelve entre otros dos problemas bases, la gestión de la infraestructura de clave pública y el problema de la ubicación de los certificados.

Gestión centralizada de usuarios y contraseñas. De esta forma es posible realizar la trazabilidad de las distintas operaciones dentro de la red.

Por estas razones es que se considera oportuno realizar la evaluación de un proyecto de implantación de un SD para el gobierno.

Alcance del Proyecto.

La Secretaría de la Gestión Pública, por medio de la Dirección Provincial de Informática, tiene como uno de sus objetivos principales definir la infraestructura tecnológica base para asegurar la integración e interoperabilidad de los recursos

tecnológicos a nivel gubernamental. Por todo ello se plantea llevar adelante un proyecto de desarrollo de la raíz del servicio de directorio para el dominio “sanjuan.gov.ar”, completando el diseño, planificación e implementación del mismo.

La finalidad es consolidar la base técnica/operativa de un servicio de directorio escalable tanto horizontal como verticalmente a nivel de gobierno. Esta raíz será la base para soportar el crecimiento de infraestructura TI de la totalidad de las áreas de gobierno.

Objetivos.

Dentro de los objetivos fijados para el proyecto propuesto se pueden definir los siguientes:

- Diseño del Servicio.
- Desarrollo del plan de ejecución.
- Desarrollo del plan de inversiones necesarias a corto y mediano plazo.
- Desarrollo del plan de RRHH.
- Obtención de la infraestructura tecnológica para consolidar el servicio.
- Migración e Integración con servicios existentes.
- Desarrollo de políticas y normativa.
- Implementación y despliegue de la solución.
- Operación del servicio.

Requerimientos.

Los requerimientos se dividen en los siguientes ítems:

- Equipamiento necesario para el montado de la raíz.
- Software - Licencia
- Consultoría para el diseño del SD global del Gobierno Provincial.
- Consultoría para el despliegue.

- RRHH a incorporar para las diversas áreas.
- Capacitación de RRHH.

Costo Total Asociado.

Este costo hace referencia a:

Esta primera etapa involucra el diseño y despliegue de la solución del servicio de directorio para consolidar la raíz del dominio “sanjuan.gov.ar”. Se adquiriría el hardware necesario para la configuración de la raíz y conectividad asociada para operar el servicio. Se capacitarán agentes de la Dirección Provincial de Informática para la administración del servicio.

El costo total estimado asociado al proyecto se detalla en la tabla que figura a continuación

Tabla de Costos

Ítem	***Detalle***	***Costo $***
1	Hardware a adquirir	50.000.-
2	Consultoría / Capacitación	15.000.-
3	Licencias	15.000.-
4	Contratos	
	Total $	80.000.-

Con este presupuesto tentativo se estima comenzar a trabajar este año para avanzar en la implantación de las bases del Servicio de Directorio del Gobierno de San Juan. Hasta el momento, el proyecto no tiene una fecha de inicio determinada,

estimándose que el mismo podrá encararse en el segundo semestre, conforme se vayan finalizando otros proyectos en curso actualmente.

SOLUCIÓN ANTIVIRUS

Ante las distintas amenazas generadas por el uso de internet y correo electrónico, surge la necesidad de contar con un servicio que brinde la protección necesaria para asegurar el correcto funcionamiento de los sistemas y garantice la continuidad de las tareas.

Esta necesidad no es exclusiva de una repartición de la administración pública sanjuanina, sino que es común a todas las dependencias que cuentan con recursos informáticos.

Para generar una homogeneidad en la resolución del inconveniente y aprovechar la fortaleza de una negociación de magnitud ante los posibles proveedores es que se decidió conformar en el ámbito de la Coordinación de Gobierno Electrónico un equipo de trabajo de especialistas conformando una Comisión Técnica. Dicha comisión se encargó de realizar un análisis de los productos existentes en el mercado que cubrieran las necesidades planteadas y brindar una posible recomendación de solución.

Los integrantes de la Comisión Técnica constituida en el ámbito del proyecto de Antivirus, cumpliendo con lo planificado por la Coordinación de Gobierno Electrónico, elaboraron un informe respecto al sistema de antivirus que se propone adoptar para implementar como solución transversal en el ámbito del poder ejecutivo provincial.

Previo a ello, se cumplió con el relevamiento de las necesidades de los ministerios de Educación, Haciendas y Finanzas e Infraestructura y Tecnología. La distribución de licencias de antivirus que abarca esta primera etapa será conforme a la tabla que se detalla a continuación.

Ministerio	Cant.

	Licencias
Infraestructura	800
Educación	700
Hacienda y Finanzas	600
Total	2.100

Es oportuno aclarar que el modo de licenciamiento que se propone solicitar es del tipo abierto. Este modo de licenciamiento, permite crecer a futuro sin necesidad de llevar a cabo procesos de adquisiciones de licencias adicionales. En el contrato de licencias, se fijan puntos de revisión, donde se blanquearán las nuevas licencias instaladas. Estos puntos suelen ser anuales, y es una buena forma de simplificar significativamente el crecimiento de la cobertura de este tipo de soluciones. Lo anterior ayuda considerablemente a la planificación de una forma más simple y ordenada de los gastos asociados a productos y servicios.

Paralelamente se elaboró un conjunto de especificaciones técnicas, para fijar una línea base referencial a la hora de evaluar diversos aspectos que determina el presente proyecto. Las mismas se adjuntan en el Anexo V.

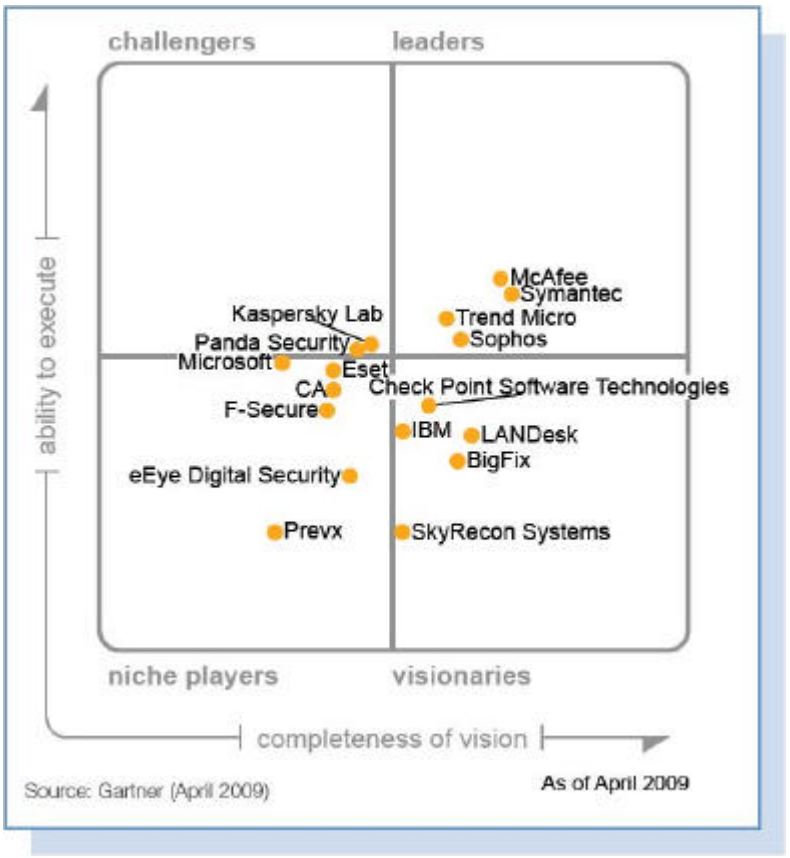
Actualmente, el estado provincial no posee la capacidad, ni los medios para llevar adelante un análisis comparativo de soluciones de antivirus. Es por ello que se decidió en profundizar el estudio de una solución ya conocida, que cumpliera con los requerimientos enunciados y evaluar el estado en que se encuentra dicha solución comparativamente en el mercado respecto de soluciones equivalentes de EndPoint Protection Plataform (Plataforma de Protección de Punto Final).

La solución tomada como base inicial para el estudio fue el producto EndPoint Protection de la empresa Symantec en su versión 11. Este producto está en uso en diversas reparticiones de la administración pública. El mismo ya fue licenciado desde hace algunos años y es actualmente la solución de antivirus que emplea la Dirección

Provincial de Informática. En base a esta experiencia, se desarrolló un laboratorio a fin de efectuar pruebas y ensayar la solución en el entorno actual del Edificio del Centro Cívico. Este laboratorio se implementó para llevar a cabo pruebas de configuración y conocer en profundidad la aplicación como solución corporativa. Complementariamente se determinó si se ajusta a los requerimientos enunciados en el anexo V. Se realizaron instalaciones en modo de prueba en los 3 ministerios mencionados.

La segunda línea de análisis fue lo referente al posicionamiento en el mercado como solución corporativa de antivirus. En diversos sitios de internet se ubica a EndPoint de Symantec como uno de los principales referentes en soluciones conocidas como EPP según sus siglas en ingles (EndPoint Protection Plataform – Plataformas de Protección para Puntos Finales). En este sentido, se puede mencionar un informe respecto al estudio de diferentes plataformas realizado por Gartner, la cual es una de las más prestigiosa consultoras internacionales. El informe analizado es el Cuadrante Mágico de Gartner para EPP en el que se analizan fortalezas y debilidades de diferentes productos existentes.

El "Cuadrante Mágico" es una forma ordenada y simple de presentar comparativamente productos disponibles en el mercado, ayudando a decidir la compra de productos o servicios Este tipo de informes es una representación gráfica de la situación del mercado de un producto/servicio tecnológico en un momento determinado.



Symantec End Point Protection SEP v. 11

Figura 1. Cuadrante Mágico para Plataformas de Protección de Punto Final

Para el análisis del Cuadrante Mágico de Gartner es importante entender su estructura. La base del mismo es la definición de dos ejes, los cuales son:

Amplitud de Visión (Completeness of Vision) Horizontal: este eje refleja la capacidad de innovación y si la empresa guía o sigue las tendencias del mercado.

Habilidad para ejecutar (Ability to Execute) Vertical: este eje resume factores tales como viabilidad financiera del vendedor, receptividad del mercado, capacidad en el desarrollo de productos, canales de ventas y base de clientes.

Para el análisis de estos ejes se involucran determinados criterios los cuales se detallan a continuación. Así los factores que contribuyen al análisis del eje horizontal, es decir el de la “Amplitud de Visión” son:

• Entendimiento del Mercado: describe a los proveedores que interpretan los requerimientos de los clientes para la defensa integrada y proactiva a través de todos los tipos de amenazas provenientes de programas malignos (malware), la

necesidad de una mejor seguridad de datos y de administración, y a aquellos proveedores con un proyecto a mediano y largo plazo innovador y oportuno para brindar dichas funcionalidades.

• Estrategia de Oferta (Producto): al evaluar las ofertas del producto de los proveedores se observan los siguientes diferenciadores de producto:

• Capacidades de Firma contra Programas Malignos (anti-malware): velocidad, precisión, transparencia e integridad de las defensas basadas en firma

• Capacidades como Sistema de Prevención de Intrusiones basadas en PC: la calidad, cantidad, precisión y facilidad de administración de defensas no basadas en firmas.

• Capacidades de Firewall Personal: las capacidades avanzadas que exceden las de Microsoft, como políticas basadas en la ubicación, VPN, reglas para redes inalámbricas, USB y tipo de protección de puertos.

• Capacidades de Administración y Reportes: Reportes detallados y centralizados que aumenten la visibilidad en tiempo real del estado de seguridad del nodo final. Además capacidades de administración, que facilitan la carga de gestión de la configuración y política. Los proveedores que se han embarcado en la integración de operación de tipo “Administración de Configuración del Ciclo de Vida de la PC” (PCLCM por sus sigla en inglés) mostraron un importante liderazgo, por lo que se les otorgó un crédito extra.

Los criterios claves de habilidad para ejecutar usados para evaluar a los proveedores en el 2009 fueron la experiencia del cliente, la respuesta del mercado y el registro de seguimiento. Se evaluaron los siguientes factores para contribuir a la dimensión vertical:

• Viabilidad General: esto incluía una evaluación de recursos financieros (como la habilidad para realizar inversiones necesarias en nuevos productos o canales) y la experiencia y enfoque del equipo ejecutivo. También se observa la estrategia de negocios de la división de protección de punto final de cada proveedor y cuán estratégica es para la compañía en general.

• Respuesta del Mercado y Registro de Seguimiento: se evalúa el registro de seguimiento de cada proveedor para ver si se han ofrecido nuevos productos y programas de alta calidad a los clientes en tiempo y forma.

• Ejecución de Ventas/ Precios: se evalúa la participación en el mercado y tasa de crecimiento de cada proveedor. También se observa la fuerza de los programas de canal, presencia geográfica, y los registros de seguimiento de éxito en sociedades comerciales o de tecnología.

• Ejecución de Mercado: se evalúa qué tan frecuentemente aparecían los proveedores en listas y RFPs, de acuerdo con las preguntas a clientes de Gartner, como así también a revisiones de canales y referencia. Asimismo, observamos presencia de la marca y visibilidad en el mercado.

• Experiencia del Cliente: en primer lugar se evalúa la estabilidad y el rendimiento del producto, la experiencia de la compañía con la asistencia del proveedor, y la calidad de firma y tiempos de respuesta. Se consideraron los comentarios y referencias de los clientes de Gartner, y a través de pruebas (como AV-Test.org) y otras fuentes de datos sobre el rendimiento y tiempos de respuesta de la firma.

• Operaciones: se evalúan los recursos de la compañía que se dedicaron a la investigación de programas malignos y producción I+D (investigación y Desarrollo)

En forma complementaria el gráfico está dividido en cuatro cuadrantes dónde se distribuyen las principales compañías en función de su tipología y la de sus productos. Los cuadrantes que se definen son:

Líderes (leaders): aquellos que tienen la mayor puntuación resultante al combinar su habilidad para ejecutar y el alcance de visión, que se refiere a su potencial.

Aspirantes (challengers): son las empresas que tienen una fuerte capacidad de ejecución. Les clasifica entre los que no tienen una fuerte propuesta de valor para los nuevos clientes. Aunque suelen tener capacidad y recursos financieros, carecen de visión, la innovación y comprensión de las necesidades del mercado. Tienen posibilidades de convertirse en líderes, si desarrollan una visión del futuro.

Visionarios (visionaries): son los que pueden tener todas las capacidades que ha de ofrecer una plataforma de EPP de forma nativa, o mediante alianzas con otros socios, lo cual significa un fuerte impulso a la integración de programas y plataformas así como una habilidad para anticiparse a las necesidades del mercado que ellos no puedan cubrir.

Jugadores de Nichos (niche players): Son las empresas enfocadas a determinadas áreas de las tecnologías EPP, pero sin disponer de una solución completa.

Así, en base a lo detallado el Cuadrante Mágico ofrece una vista instantánea del mercado, tendencias, madurez y participantes basadas en productos.

Según la consultora Gartner, Symantec mantiene la mayor participación del mercado de protección de punto final, y su producto principal, (Symantec AntiVirus (SAV)), sufrió una revisión general en el 2007 y recibió el nombre de Symantec Endpoint Protection (SEP) v 11.0. Symantec sigue siendo líder en este análisis por sus importantes mejoras en el SEP, sus capacidades de protección de fuga de datos, y planes de integración de PCLCM con Altiris. Symantec es una excelente inclusión para cualquier empresa de alcance global, especialmente aquellas que aprecian el valor de la integración PCLCM y EPP.

Fortalezas

• Una parte significativa (25%) de su base instalada ha migrado y probado SEP 11.0, y el producto se encuentra en su cuarto paquete de mantenimiento.

• La nueva interface de administración y notificación basada en tecnología Sygate, representa una importante mejora a la vieja versión SAV. Está orientado a tareas y ofrece sus importantes mejoras en cuadros de controles de notificaciones y utilización.

• El motor contra programas malignos (malware) ha sido mejorado con la incorporación del sistema de seguridad personal Sygate, protección de puerto y dispositivo, y NAC mejorado en una arquitectura de agente único. El nuevo agente tiene una huella más pequeña debido a la consolidación de agente, y brinda las velocidades de escaneo más rápidas en pruebas recientes (AV-Comparatives.org).

Symantec también agregó un número de programas para minimizar el impacto de escaneos programados.

• La protección de programas malignos ha sido ampliada con más capacidades de prevención HIPS (Sistema de Intrusión basada en host) y mayor precisión de detección.

• Symantec también ofrece backup de datos y tecnología de accesos remotos, y tecnología de imágenes, con las marcas Veritas y Ghost. Sin embargo, dichas tecnologías no han llegado al conjunto EPP o la consola administrativa.

• La compra de Altiris de Symantec será muy importante ya que continúa la integración con PCLCM. Symantec podrá aprovechar la funcionalidad de PCLCM, como el bien descubrimiento/inventario, administración de configuración, evaluación de vulnerabilidad, y capacidades de administración y distribución de software

• Symantec ha hecho inversiones significativas en DLP (Prevención de Pérdida de Datos), y ofrece un agente DLP para el cliente como parte del conjunto Vontu DLP

• Symantec cubre un amplio rango de puntos finales, incluyendo Windows Mobile, Symbian, Palm, Linux y Mac

• El motor de flujo de trabajo Symantec que le permite a las organizaciones automatizar sus procesos de seguridad y operaciones, brinda una buena solución a las organizaciones que quieren integrar aplicaciones dispares a procesos repetitivos de operaciones y seguridad

Advertencias

• Symantec todavía recibe críticas de sus clientes por el soporte y servicio. La dirección se está ocupando de estos problemas, pero llevará tiempo implementar mejoras. Los grandes clientes deberían exigir que ingenieros en soporte sean asignados a sus cuentas.

• A pesar de las mejoras, Symantec se orienta a la calidad y testeo de código porque SEP 11.0 presentó numerosos problemas en su lanzamiento. Sin embargo, el paquete de servicio MR3 lanzado en septiembre de 2008 ha resuelto la mayoría de estos puntos.

• Los requisitos de recurso y rendimiento del servidor administrativo son un problema para las pymes. La edición Small Business lanzada en el 2009 se enfocará en la facilidad de uso, cuadro de controles y notificaciones de estado simplificados, mejoras en el rendimiento del servidor administrativo y uso de recursos, y licencias de suscripción.

• El SAV para la modernización de SEP es un importante emprendimiento que exige a los usuarios reemplazar la infraestructura de agente y administración. También requiere entrenamiento para la nueva consola administrativa y las opciones de configuración expandida. Symantec ha aumentado sus recursos para que esta transición sea más suave con el despliegue de numerosas guías y soporte.

• Symantec debe manejar cuidadosamente la integración del entorno administrativo Altiris, y debería publicitar su mapa de ruta para que la estrategia de migración sea clara para clientes actuales y futuros.

• Las soluciones Altiris Patch Management y la administración de vulnerabilidad son muy débiles.

• Symantec carece de soporte Windows Server 2008.

• Symantec todavía carece de su propia encriptación de archivo o de disco completo, aunque tiene licencia GuardianEdge. DLP se ha integrado con la consola administrativa Altiris, mientras que la codificación GuardianEdge está integrada con la administración SEP, complicando la protección de datos. Se espera que Symantec adquiera un proveedor de codificación en el 2009

• La consola convergente de administración y funcionalidad SEP 11.0 no se extiende a clientes Mac o Linux, o a sus pasarelas de e-mail y Webs.

• La sobre posición con Symantec Critical System Protection y Symantec Control Compliance debe ser racionalizada y consolidada en una única consola de notificación y administración.

• No está integrada la tecnología de Buffer overflow de Sygate. La mayoría de los competidores EPP ofrecen protección de Buffer overflow.

Aclaraciones

Es importante aclarar que a partir de las advertencias presentadas en el presente informe, surgen consideraciones a tener en cuenta a la hora de la redacción de las especificaciones técnicas para la adquisición. Un punto a considerarse es el que Symantec carece de soporte a Windows Server 2008. Se realizaron las averiguaciones correspondientes, así a partir del lanzamiento del MR5 (http://aka-community.symantec.com/connect/pt-br/articles/new-features-ru5-mr5)
SEP ya brinda soporte a esa versión de operativo.

Otra consideración importante del informe de Gartner es la recomendación de incrementar los requerimientos respecto al soporte que debe tener el gobierno de San Juan sobre una solución de Protección de Punto Final. En especial la solicitud de la asignación de un ingeniero de soporte a la cuenta de Gobierno.

El producto de Symantec está dentro del cuadrante denominado “Líderes”. En este cuadrante se ubican aquellas empresas que demostraron un progreso y esfuerzo equilibrados en todas las categorías de ejecución y visión referidas a las soluciones de EPP. Las empresas ubicadas en este cuadrante enfocaron sus acciones en la protección contra programas malignos avanzados, protección de datos y/o capacidades administrativas lo cual conduce a elevar el nivel competitivo del mercado, y pueden cambiar el curso de la industria.

El producto Endpoint Protection de Symantec es uno de los mejor posicionados, en lo referente a visión de mercado y capacidad de ejecución como empresa en soluciones EPP.

Otro producto analizado fue ForeFront de Microsoft. El análisis se efectuó sobre una propuesta presentada por la firma NEC de la solución de EPP basada en este producto. Del análisis efectuado en base a los requerimientos presentados en el Anexo V, dos puntos fueron valorados como negativos. Los puntos corresponden a la falta de soporte para ambientes operativos del tipo LINUX o distintos a Windows y su condición de ser uno de los productos más nuevos del mercado. Esto resulta un punto en contra con la solución de Symatec que sin dudas es una de las más antiguas y con mayor trayectoria, cumpliendo además con la totalidad de lo enunciado en el Anexo V.

Por lo antes expresado es que la comisión resolvió proponer que se adopte el producto Endpoint Protection de la firma Symantec, en su última versión liberada al momento de la adquisición, como solución corporativa de antivirus para ser adoptada en el ámbito del Poder Ejecutivo Provincial. En forma complementaria se aconsejó extender el licenciamiento actual del producto de Symantec, EndPoint Protection para cubrir la totalidad de las licencias necesarias.

En este momento, habiéndose aprobado el informe correspondiente se realizó un llamado a licitación pública para fines de abril en donde se procederá a analizar las diferentes propuestas y adoptar la más conveniente para la provincia.

SERVICIO DE CORREO ELECTRÓNICO

Uno de los proyectos llevados adelante durante la última parte del año 2010 fue la migración de las cuentas de correo electrónico oficial “sanjuán.gov.ar”. El Servicio de Correo Electrónico se encontraba en un Servidor pago de WebHosting (TOWEBs) y se decidió migrar todas las cuentas a Servidores propios de Exchange que tiene el Ministerio de Educación. Al momento de la migración, se tenía un total de 568 buzones de los cuales se disponía muy poco conocimiento de quien eran los usuarios que usaban correo. Por lo tanto, se propuso hacer un relevamiento y depuración de todas las cuentas.

Inicialmente se realizó la capacitación del personal para atender una Mesa de Ayuda y preparar una serie de instructivos para publicar en un micro sitio. Para ello, se conformó un equipo de trabajo con personal de la Dirección de Informática, del Ministerio de Educación y la firma NEC para realizar la migración.

Relevamiento y depuración

Para comenzar, se encararon las tareas de relevamiento, clasificación, depuración y verificación de todas las cuentas de correos existentes. Esta tarea demando un tiempo considerable ya que había que ubicar a cada usuario de los cuales en muchos casos se disponía únicamente del nombre de la cuenta. Se empezó relevando los datos de las planillas de solicitudes de altas de cuentas existentes y se agregaron a una planilla de Excel con datos que se tenía previamente. Se tomo la planilla y se clasificó por ministerios y secretarias se marcaron las cuentas invalidas. Por cada cuenta de correo existente se verificaron los datos personales contactando a la persona o algún responsable por teléfono o personalmente y se lo marcaba como válida la cuenta. En la última etapa se contactó con cada unidad Ministerio, Secretaria, Dirección y se verificó que la cuenta quede configurada en un cliente de correo para no perder piezas de correo.

La siguiente tabla muestra los valores antes de la Migración

TOTAL de cuentas en ToWebs	568
cuentas depuradas [70%]	398
cuentas de desconocidos [22 %]	127
cuentas eliminadas [8 %]	43

Mesa de Ayuda e Instructivos

Con personal de la DPI, se realizó una capacitación sobre una serie de conceptos necesarios para atender la Mesa de Ayuda que dará soporte en el primer nivel en materia del nuevo Servicio de Correo. En este sentido, se habilitó un Interno 6800 para atender los llamados. Además, se prepararon guías que instruyen sobre cómo configurar una cuenta de correo en un cliente local, material sobre el uso Outlook Express y para administrar e importar libreta de direcciones. También se creó un pequeño micro sitio en la página de Gobierno para publicar toda la información que se disponía.

Todo esto se acompañó con una serie de correos masivos a las cuentas sin identificar donde se solicitaba a los usuarios que se reportasen a la Mesa de Ayuda. Finalmente, antes y después de la migración se realizaron tareas de configuración de las pc's de los distintos ministerios para que no se pierdan las piezas de correo.

Equipo de Trabajo

Conjuntamente con el Ministerio de Educación y personal de NEC se definieron los procesos para la realizar la migración. Primero se instaló una consola de Administración en un Servidor del Ministerio de Educación con Windows 2003 server y en la DPI se preparó una Pc con Windows XP para que se conecte a consola. La unidad tecnológica hizo el enrutamiento para que sea segura la

conectividad al realizar el acceso. Se crearon los usuarios en la consola y se empezó a realizar las pruebas de creación de cuentas en una Unidad Organizativa propia del servicio de Active Directory para Gobierno. Se establecieron las políticas para estas cuentas como también se definieron los tamaños de los Buzones. Faltando unas semanas para la migración se dejó de crear cuentas en TOWEBs y se empezó a preparar el archivo para realizar las altas de las cuentas en el nuevo ambiente.

Finalmente, el día 20 de Agosto se cruzaron los archivos con el de las claves y se dieron de Alta con éxito las 568 cuentas después de resolver algunos problemas con cuentas dobles y nombres repetidos. Se reactualizaron todos los DNS y los Certificados para que empiece a redirigir todos los correos que llegaban al dominio sanjuán.gov.ar y sanjuán.gob.ar a los nuevos servidores de Exchange. En tanto que el servicio en Towebs se dejo accesible para aquellos usuarios que no habían bajado su correo a su pc y poder recuperarlos.

Después de la Migración

Las semanas posteriores se empezaron a recibir reportes de distintas incidencias que ocasionó toda la migración y se empezó a resolver los problemas. Dichas incidencias variaban desde problemas en las configuraciones en los equipos hasta nuevos requerimientos de conectar los equipos de BlackBerry para leer el correo en el celular. Para ello, se elaboraron una serie de instructivos para administrar los nuevos servidores y documentar errores. Las tareas que continuaron después de la migración fueron tantas como antes y consistieron, principalmente en brindar soporte a los administradores y usuarios del correo. Se tuvo que aprender a Administrar la consola del Correo Exchange y armar comandos para evaluar datos estadísticos con la consola Power Shell. Se confecciono el Skin de gobierno para ingresar al Servicio del Owa, el acceso desde la Pagina Web. Se definieron los procesos para las Altas de las Cuentas como también el circuito que involucraba la Mesa de Entrada de la Secretaria de Gestión Pública y Recursos Humanos. De esta forma, se empezó a usar un nuevo Formulario de Solicitud de correo.

A la fecha se puede afirmar que el servicio de correo se encuentra estabilizado y está siendo administrado en servidores del gobierno por empleados de la administración pública sanjuanina, dejando de lado la dependencia de terceros en esta materia.

Asimismo, este servicio permite un importante ahorro en materia de utilización de ancho de banda, ya que los correos entre cuentas del gobierno que anteriormente eran ruteados a un servidor en Buenos Aires, actualmente resuelven en forma local dentro del ámbito de la misma red provincial.

HOSTING DE SITIOS WEB

Situación Actual

El portal principal del Gobierno de la Provincia de San Juan, cuya dirección en internet es la siguiente: http://www.sanjuan.gov.ar; se encuentra alojado actualmente en servidores pertenecientes al Consejo Federal de Inversiones CFI). Este portal fue desarrollado en tecnología ASP.NET y la dirección de Internet en donde se encuentra esta aplicación es: http://sanjuan.cfired.org.ar/

El principal problema radica en que existe un número importante de sitios pertenecientes a ministerios, direcciones, programas y otras instituciones, que se encuentran disponibles en sub-dominios de sanjuan.gov.ar . Por ejemplo:

Ministerio de Producción

http://produccion.sanjuan.gov.ar

Cada uno de estos diferentes sub-dominios -por lo general- contiene una aplicación, sistema, CMS, o pagina web estática.

Todos estos sub-dominios y otros sitios adicionales se encuentran alojados actualmente en servidores pertenecientes a la empresa ToWebs con las siguientes características:

Directorios/Sub-dominios:	84
Espacio utilizado:	30Gb
Trasferencia web:	57747 MB
Transferencia FTP:	197 MB
Mysql	21 bases de datos

Sistemas CMS y aplicaciones:

Joomla 1.5.x	(10 sitios)
Movable Type 2.63	(1 sitio)
Sitios PHP/MySQL programados a medida	(8)

Algunas definiciones y conceptos necesarios

Joomla!

Joomla! es un sistema de gestión de contenidos, y entre sus principales virtudes está la de permitir editar el contenido de un sitio web de manera sencilla. Es una aplicación de código abierto programada mayoritariamente en PHP bajo una licencia GPL. Este administrador de contenidos puede trabajar en Internet o intranets y requiere de una base de datos MySQL, así como, preferiblemente, de un servidor HTTP Apache.

En Joomla! se incluyen características como: mejorar el rendimiento web, versiones imprimibles de páginas, flash con noticias, blogs, foros, polls (encuestas), calendarios, búsqueda en el sitio web e internacionalización del lenguaje. Su nombre es una pronunciación fonética para anglófonos de la palabra swahili jumla, que significa "todos juntos" o "como un todo". Se escogió como una reflexión del compromiso del grupo de desarrolladores y la comunidad del proyecto.

Componente K2

K2 es un potente componente de contenido para Joomla! con funcionalidades similares de CCK (Content Creation Kit – Kit de Creación de Contenido) desarrollado por la empresa JoomlaWorks. Esta extensión provee una solución integrada contemplando formularios ricos de contenido para los items (Los ítems se llaman a los viejos Artículos de Joomla! pero que además poseen galerías de imágenes, videos, adjuntos, campos extra, entre otros), árbol de categorías ilimitado en sub-niveles, tags, comentarios, un sistema de campos adicionales extra (similar a CCK en Drupal) para extender la base de los ítems. K2 posee también una API para extender los ítems, categorías y formularios de usuarios, ACL, edición desde frontend, sub-plantillas y mucho más.

Al usar K2, se pueden transformar los sitios web en Joomla! a sitios de noticias, revistas, con blogs de autores, catálogos de productos, portfolio de trabajos, base de conocimientos, administradores de documentos/archivos, listado de directorio, eventos, y mucho mas. Desde que K2 se puede extender con campos

adicionales, se puede fácilmente crear tipos de contenido específicos a categorías, por ejemplo artículos, posts de blogs, pagina de producto, listado de directorio.

Funcionalidades de K2

Anidamiento de Categorías

K2 permite olvidar el viejo sistema de administración de contenido de Joomla! en donde solo se contemplan la posibilidad de tener una o más categorías bajo una sección de contenido, lo que implica un árbol de contenido de 2 niveles.

Micro-plantillas

K2 permite generar micro plantillas de diseño que pueden ser asignadas a categorías diferentes. Por ejemplo, se pueden tener 2 plantillas, una “contenido” y otra “blog” en donde cada plantilla posee un diseño y un esquema diferente, y cada una de estas asignarse a categorías de contenido diferentes

Tagging

Permite la asignación de tags a cada ítem de contenido, en la forma de enlaces, los cuales pueden generar luego un catalogo de información.

Flexibilidad de Diseño

Cada categoría de contenido posee su propio esquema o distribución. Además posee una serie de opciones que pueden ser activadas o desactivadas, lo que sumado a la funcionalidad de micro plantillas brinda un enorme abanico de posibilidades en cuanto al diseño.

Control Extendido de Usuario

K2 permite importar los datos de usuarios existentes en el sitio Joomla! especifico. Una vez importados, estos usuarios se pueden asignar a grupos de

usuarios K2, y al mismo tiempo definir roles y opciones, lo que genera un sistema básico de ACL (Access Control Lists o Listas de Control de Acceso). Esta funcionalidad permite asignar diferentes permisos a diferentes grupos de usuarios. Estos grupos de usuarios son luego asignados a las categorías disponibles. Por ejemplo: los usuarios del un grupo especifico sólo pueden escribir artículos en la categoría “blog”.

Soporte

Existe una amplia comunidad de usuarios, foros y listas de correo relacionadas a K2 en donde se pueden encontrar soluciones a los diferentes problemas que se encuentren.

El componente K2 es gratuito, es decir no tiene costo alguno y puede obtenerse a través de http://getk2.org y http://es.getk2.org

Proyecto de migración de sitios y consolidación de una estructura única

En la actualidad se está analizando el desarrollo de un proyecto que permita lograr los siguientes objetivos:

- Migrar el dominio sanjuan.gov.ar por completo a los servidores del Consejo Federal de Inversiones. La meta fundamental es “eliminar” la redirección actual que se produce:

  http://sanjuan.gov.ar => http://sanjuan.cfired.org.ar

- Migrar cada una de los sitios, páginas estáticas y aplicaciones web contenidas en el Hosting actual y sub-dominios a los servidores del Consejo Federal de Inversiones.
- Migrar bases de datos, usuarios de bases de datos, perfiles y permisos desde un servidor hacia otro.

Para todos los sitios desarrollados en Joomla! existe un grupo separado de objetivos y tareas a desarrollar:

- Migrar cada sitio en Joomla! al nuevo servidor y verificar su perfecto funcionamiento.
- Actualizar a la última versión: En donde sea posible, actualizar y convertir cada sitio a Joomla! 1.6.1, actualizando tanto contenido, como así también realizando la conversión de formato de la plantilla correspondiente que el sitio este utilizando. De no ser posible una conversión y actualización a Joomla! 1.6.1, actualizar dicho sitio a la última versión de Joomla! de la rama 1.5.x.

  En caso de que algún sitio Joomla! no pueda ser convertido a Joomla! 1.6.x, instalar, configurar y optimizar el componente K2 -descripto anteriormente- en cada uno de los sitios Joomla! y realizar las tareas pertinentes para que en cada uno de estos sitios K2 sea el sistema principal de administración de contenidos. Ésto implica migrar contenido actual tanto artículos, secciones y categorías, migrar usuarios, crear grupos de usuarios, perfiles de acceso y configurar las opciones de cada categorías K2.
- Elaborar un documento tutorial donde se explique en general la administración del componente K2 desde el frontend de cada sitio Joomla!. Este documento será remitido a cada uno de los administradores del sitio Joomla! para que aprendan a administrar el contenido con este nuevo sistema y puedan además involucrarse con todas las ventajas que este incorpora.
- Verificar todos los links existentes y emitir reportes detallados de links que no se encuentren funcionando o apunten a destinos inexistentes (Error 404) y en lo posible intentar resolverlos.
- Emitir un reporte detallado resultante de un análisis exhaustivo de cada sitio en Joomla! contra spyware, malware y otros tipos de troyanos y/o exploits que puedan encontrarse. Resolver cada uno de estos inconvenientes y emitir un reporte final donde se puedan corroborar los

cambios efectuados para que el sitio se encuentre protegido contra ataques e infecciones.

- Realizar en cada sitio Joomla! un informe detallado sobre SEO (Search Engine Optimization => Optimización en Buscadores) y proponer para cada uno de estos sitios una serie de tareas a realizar para lograr un posicionamiento óptimo (en lo posible a corto plazo) de cada uno de estos sitios Joomla!.
- Una vez finalizadas las tareas de remoción de virus, tareas de SEO y verificación de links rotos, etc. realizar y proponer una serie de tareas o herramientas a instalar y configurar para poder proteger cada uno de estos sitios contra ataques, exploits y otra serie de amenazas.

La idea principal del proyecto es integrar los distintos sitios en un solo ambiente y que la instalación, configuración y ejecución de estas herramientas no genere un impacto negativo en la performance de cada uno de ellos.

Se estima que para el mes próximo se estará avanzando en este proyecto que se estima de una duración aproximada de un mes.

CONCLUSIONES

Como puede apreciarse en el presente informe y en anteriores, son muchos los proyectos y tareas que se desarrollan en la Dirección Provincial de Informática de la Provincia de San Juan.

El objetivo principal de dichos proyectos es el de generar un ámbito profesional adecuado en la provincia para el desarrollo del gobierno electrónico tratando de potenciar a los recursos propios y minimizando la dependencia de terceros.

En este sentido se han llevado a cabo numerosas actividades a partir la creación de un ámbito de trabajo coordinado a través de la Coordinación de Gobierno Electrónico que permitió ahorrar esfuerzos y generó una sinergia entre las distintas áreas del gobierno.

Así fue posible encarar distintos proyectos como los de adquisición de la solución antivirus y correo electrónico que están en plena ejecución y preparar otros como la implantación de una aplicación para la gestión de expedientes para toda la administración pública.

Mucho es lo que se ha hecho, pero es mucho lo que todavía falta por realizar. En este sentido se ha dado un paso fundamental en la generación de una cultura de trabajo cooperativo entre los recursos de la administración pública centrado en la necesidad de capacitación y actualización de conocimiento de los mismos.

Se espera, en los próximos meses poder avanzar con la definición de una integración de todas las redes, el control y monitoreo de esta estructura por parte del personal de la administración pública y el desarrollo e integración de aplicaciones y bases de datos que puedan ser utilizadas como herramientas por todas las reparticiones que lo requieran.

ANEXOS

ANEXO I

REGLAMENTO INTERNO DE FUNCIONAMIENTO, MANTENIMIENTO Y CONSERVACION DE LAS INSTALACIONES DEL EDIFICIO GUBERNAMENTAL CENTRO CIVICO

CAPITULO I
DISPOSICIONES GENERALES y AUTORIDAD DE APLICACION

ARTÍCULO 1º.- El presente reglamento tiene por objeto establecer la normativa para el funcionamiento, mantenimiento y conservación de las instalaciones que conforman el edificio Centro Cívico, fijando los lineamientos para quienes hagan uso de las mismas y contribuyan a generar un clima laboral armónico.

ARTICULO 2º.- El edificio Centro Cívico comprende todo el inmueble ubicado en Avenida Libertador General San Martín 750 (Oeste) de la Ciudad de San Juan, que se describe en el Anexo II del presente, con sus instalaciones internas y asimismo todas las mejoras que se le hicieren en el futuro.

ARTÍCULO 3º.- Este reglamento será de aplicación para todos los funcionarios , para los empleados que cumplan funciones en forma efectiva en la Administración Pública Provincial bajo cualquier modalidad, para el personal de empresas privadas que realicen cualquier tipo de tareas en el edificio y como así también para todo público en general que utilice o ingrese a las instalaciones. En caso de violación a lo normado por la presente será de aplicación el Régimen Disciplinario que fuere vigente, y demás normas penales y correccionales de la provincia de San Juan.

ARTÍCULO 4º.- El Ministerio de Infraestructura y Tecnología, a través de las áreas bajo se dependencia, será el organismo responsable del Mantenimiento de la estructura edilicia del Centro Cívico, pudiendo previo dictado de acto administrativo, instrumentar remodelaciones al edificio.

ARTICULO 5°.- La Subsecretaría de Planificación y Control de Gestión dependiente del Ministerio de Infraestructura y Tecnología, a través de la Dirección de Control Operativo, tendrá la responsabilidad del cuidado, seguridad, control, uso y conservación del edificio Centro Cívico de acuerdo a las pautas establecidas en el presente Decreto.

ARTICULO 6º.- La Secretaría de la Gestión Pública dependiente del Ministerio de Hacienda y Finanzas, tendrá a su cargo la responsabilidad de la capacitación y divulgación del presente reglamento. Asimismo, instrumentará un programa de capacitación y sensibilización tendiente a lograr un adecuado uso de las instalaciones y a alcanzar conveniente un clima de convivencia laboral.

ARTICULO 7°.- Facúltese a la Subsecretaría de Planificación y Control de Gestión dependiente del Ministerio de Infraestructura y Tecnología conjuntamente con la Secretaría de la Gestión Pública dependiente del Ministerio de Hacienda y Finanzas a elaborar y dictar las normas técnicas complementarias o aclaratorias relativas al ordenamiento establecido por el presente Decreto.

CAPITULO II

DE LA SEGURIDAD, ACCESOS Y CIRCULACIÓN POR EL EDIFICIO CENTRO CÍVICO

ARTÍCULO 8º.- El sistema de seguridad del edificio estará a cargo de personal de vigilancia de la Dirección de Control Operativo y personal de la Policía de la Provincia de San Juan, quienes cumplirán sus funciones en el destacamento localizado en el primer subsuelo del Centro Cívico. La Dirección de Control Operativo deberá inspeccionar, observar, coordinar y ordenar todas las acciones inherentes al mantenimiento del orden y la seguridad, dando intervención a la policía

de la Provincia en los casos que observare algún hecho ilícito contemplado en la normativa penal y contravencional vigente.

ARTICULO 9º.- La Dirección de Control Operativo será la encargada del funcionamiento y operatividad del sistema de cámaras de video ubicadas en la sala de monitoreo del edificio debiendo respetar lo estipulado por la Ley Provincial Nº7902.

ARTÍCULO 10º.- El personal de vigilancia de la Dirección de Control Operativo, el desarrollo de sus funciones, deberá portar el uniforme con credencial identificatoria.

ARTÍCULO 11º.- Quedan establecidos tres tipos de áreas en el edificio Centro Cívico, definidas por su nivel de accesibilidad, a saber:

Acceso Prohibido: Áreas a las que sólo puede acceder personal autorizado por la Dirección de Control Operativo. Las áreas de acceso prohibido son:

Azotea

Sala de máquinas

Centro de Control Operativo

Acceso Restringido: Áreas a las que solo se puede acceder con autorización de los responsables directos de cada una de ellas. Las áreas de acceso restringido son:

Auditorio

Salón Cruce de los Andes

Estacionamiento

Centro de Cómputos de la Dirección Provincial Informática.

Cuarto de Cableado

c) Acceso Público: Áreas no citadas en los incisos anteriores, que son de libre acceso y circulación en los horarios pre-establecidos a todo efecto.

ARTÍCULO 12º.- Se establecen dos bandas horarias por razones de operatividad:

Banda Horaria Abierta: Lunes a Viernes de 06:30 horas a 21.30 horas. De libre circulación al público en general y con las restricciones establecidas en el artículo anterior. El horario de atención al público podrá ser fijado por cada una de las reparticiones públicas dentro de esta banda horaria, según las necesidades y la normativa que le sean de aplicación. En caso de ampliación de esta banda horaria cada Repartición deberá notificar con antelación a la Dirección de Control Operativo, para que tome los recaudos necesarios a tal efecto.

b) Banda Horaria Cerrada: lunes a viernes de 21:30 horas a 06.30 horas, y todo el día sábados, domingos y feriados. En este horario sólo podrán ingresar funcionarios de rango superior y personal previamente autorizado.

ARTÍCULO 13º.- Se fijan como pautas de acceso al Centro Cívico, conforme a las bandas horarias transcriptas las siguientes:

-En Banda Horaria Abierta: de 6,30 horas a 13,30 hs estarán habilitados todos los accesos para ingreso y egreso a toda personas, y de 13,30 a 21,30 horas sólo permanecerán disponibles para el ingreso los accesos ubicados sobre Plaza Seca, Avenida Libertador San Martín y Avenida Ignacio de la Rosa.

- En la Banda Horaria Cerrada: todos los accesos permanecerán cerrados, pudiendo ingresar solo el personal autorizado y por el acceso ubicado en Avenida Libertador San Martín, donde se llevará a cabo un registro expreso por parte del personal de seguridad.

ARTÍCULO 14º.- Será facultad de los responsables del control del edificio cerrar todas las vías de acceso, cuando fuere necesario para preservar la integridad de las personas que se encuentran en su interior, o bien para resguardar la infraestructura en general Debiendo respetarse en todo momento las salidas de emergencia las cuales no podrán ser obstruidas bajo ningún aspecto.

ARTÍCULO 15º.- La Dirección de Control Operativo será responsable de aplicar los controles y medidas necesarias para hacer cumplir las restricciones de acceso establecidas en los artículos anteriores.

ARTÍCULO 16º.- El personal que deba ingresar en áreas restringidas y/u horarios restringidos deberán contar con autorización otorgada por la Dirección de Control Operativo.

ARTÍCULO 17º.- Las áreas de uso común del edificio, tales como pasillos, salas de reunión, puertas, escaleras, ascensores y otros, no podrán ser obstruidas por materiales de trabajo, mobiliario, equipo o cualquier otro elemento similar.

ARTÍCULO 18º.- Se establece que toda visita guiada que se efectuare en el edificio Centro Cívico deberá ser previamente autorizada por la Dirección de Control Operativo, a quien se lo faculta para fijar los procedimientos a seguir a tal efecto.

ARTÍCULO 19º.- La salida del edificio de bienes de propiedad del estado provincial solo podrá llevarse a cabo previa información a la Dirección de Control Operativo, quien deberá proveer un formulario por duplicado, quedando el original para la citada Repartición y la copia para el organismo de pertenencia.

ARTICULO 20º.- Los funcionarios y/o agentes que ingresen y egresen diariamente con algún equipo informático sea de su propiedad o del Estado

Provincial, deberán previamente declararlo a la Dirección de Control Operativo bajo el procedimiento que se fije a tal efecto.

ARTÍCULO 21º.- Queda prohibido realizar dentro del Edificio Centro Cívico toda actividad comercial que no fuere debidamente autorizada por parte de la Dirección de Control Operativa.

ARTÍCULO 22º.- Queda prohibido el acceso al edificio de toda persona que se encuentre en estado de ebriedad, bajo efectos de droga, enervante o con sus facultades evidentemente alteradas. Asimismo las personas que se encuentren dentro del edificio, y no guarden la compostura debida o causen molestias a usuarios o público en general, podrán ser desalojadas por parte del personal policial, pudiendo ser de aplicación las medidas penales o administrativas que correspondieren.

ARTICULO 23º.- Queda prohibido el ingreso de animales, con excepción de aquellos que acompañen a las personas en su función de guía.

ARTICULO 24º.- Las áreas de acceso y salida vehicular del edificio y los estacionamientos, contarán con la señalización correspondiente, de acuerdo a las normas establecidas en materia de seguridad pública y de protección civil vigente.

CAPITULO III

DEL FUNCIONAMIENTO Y MANTENIMIENTO DE LAS INSTALACIONES

ARTÍCULO 25º.- Los requerimientos de mantenimiento preventivo o correctivo, de remodelación de todas las instalaciones y de cualquier servicio que se necesite para el buen funcionamiento del edificio deberá solicitarse a la Dirección de Control Operativo de acuerdo al procedimiento que para tal fin establezca, quedando prohibido a los agentes públicos y funcionarios de todas las dependencias efectuar cualquier reforma o reparación por iniciativa propia.

ARTÍCULO 26º.- La coordinación de la limpieza en los espacios comunes del Centro Cívico estará a cargo de la Dirección de Control Operativo, quien confeccionará un programa específico a fin de obtener la máxima eficiencia sin entorpecer los servicios que se otorgan en el edificio.

ARTÍCULO 27º.- Se establece que la limpieza de oficinas y dependencias internas estará a cargo de personal perteneciente a cada Repartición u organismo.

ARTÍCULO 28º.- El manejo de cargas de elementos o materiales que ingresen al Edificio deberá ser autorizado previamente por la Dirección de Control Operativo, que indicará el recorrido y forma de traslado de las mismas. Cuando la magnitud de la carga ocupe más de un lugar asignado a tal fin o pueda llegar a obstruir el normal desarrollo de las actividades, se deberá realizar exclusivamente en horario de13,30 horas a 21,30 horas.

ARTÍCULO 29º.- La Dirección de Control Operativo tendrá a su cargo la recepción de toda la correspondencia que ingrese al edificio y deberá dar oportuno aviso a las áreas destinatarias para su retiro.

ARTÍCULO 30º.- Las Salas de Reunión y Conferencia existentes en cada piso, serán de uso común a todos los Ministerios, debiéndose coordinar su uso y disponibilidad según el procedimiento establecido por la Dirección de Control Operativo.

ARTÍCULO 31º.- Los espacios internos y externos de uso común del edificio Centro Cívico podrán ser utilizados para la realización de eventos, previa requerimiento mediante expediente y autorización de la Dirección de Control Operativo.

Para su autorización se deberá tomar en cuenta:

a) Importancia y características del evento en cuestión.

b) Funcionalidad del espacio requerido para realizar la actividad.

c) Labor diaria de los agentes públicos y usuarios en general.

d) Seguridad del edificio y sus usuarios.

e) Figura arquitectónica del edificio.

ARTÍCULO 32º.- Será de competencia para la distribución de los lugares de estacionamiento de jurisdicción del Poder Ejecutivo Provincial, tanto dentro como afuera del edificio Centro Cívico, el Ministerio de Infraestructura y Tecnología. El estacionamiento será con destino exclusivamente para el personal jerárquico que componen los distintos Ministerios de Gobierno. La Dirección de Control Operativo es la encargada del control de las áreas dedicadas al estacionamiento del parque automotor, quien asignará los espacios llevando el registro de los vehículos, sus responsables y los horarios autorizados. En banda horaria cerrada pueden ser solo guardadas las movilidades oficiales en las dársenas de estacionamiento libres, respetando los espacios asignados a cada ministerio.

ARTÍCULO 33º.- Queda prohibido fumar dentro de las instalaciones del edificio gubernamental Centro Cívico en estricta concordancia con lo estipulado por Ley Provincial Nº 7.595, como así también el encendido de todo producto que emane humo y que pudiera accionar el sistema de sensores contra incendio que posee el edificio.

CAPITULO IV

DE LA CONSERVACION DE LAS INSTALACIONES

ARTÍCULO 34º.- Los funcionarios y demás personal que cumplan funciones en forma efectiva dentro del Centro Cívico bajo cualquier modalidad, personal de empresas privadas y público en general están obligados a procurar la conservación de las instalaciones del edificio Centro Cívico tanto en su área de trabajo como en todo el edificio en general, debiendo reportar en forma inmediata cualquier irregularidad a la Dirección de Control Operativo.

ARTÍCULO 35º.- Cada Repartición Pública instalada en el Centro Cívico que necesite reorganizar sus mobiliarios y equipos dentro del edificio, deberá previamente comunicar a la Dirección de Control Operativo a fin de que se instrumente los recaudos necesarios para la correcta disposición de las redes eléctricas, de computación y de telefonía pre-existentes.

ARTICULO 36º.- Las remodelaciones que a futuro deban realizarse en el edificio, se efectuarán respetando la arquitectura del edificio y de acuerdo a la opinión expresa que al respecto emita el Ministerio de Infraestructura y Tecnología.

ARTÍCULO 37º.- Queda prohibido el pegado de papeles, afiches, folletería, almanaques, fotografías, guías telefónicas y cualquier otro elemento de características similares sobre la tabiquería, paredes y mobiliario existentes en el edificio. La Dirección de Control Operativo proveerá el mobiliario uniforme para que cada Ministerio cuente con un sistema de cartelera para el manejo de su información.

ARTÍCULO 38º.- Con el objeto de ornamentar o personalizar el área de trabajo solo se podrán colocar cuadros, relojes u otra representación artística del lado interno de los paneles divisorios de las respectivas áreas de trabajo. Los mismos deberán estar enmarcados y respetar el modelo arquitectónico del edificio. Para este efecto se utilizarán adhesivos de contacto o sistemas colgantes.

ARTÍCULO 39º.- El mobiliario que se ingrese a las dependencias del edificio deberá ser previamente autorizado por el Ministerio de Infraestructura y Tecnología, a través de sus órganos de competencia, a los fines de preservar el estilo y diseño acorde con el existente.

ARTÍCULO 40º.- Las dependencias de trabajo de los Ministerios o Secretarías de Estado que requieran mantenimiento o reparación de su mobiliario o de las instalaciones edilicias deberán solicitarlo previamente a la Dirección de Control Operativo, quien lo llevará a cabo dentro de un plan de mantenimiento correctivo.

ARTICULO 41º.- La Dirección de Control Operativo realizará periódicamente auditorías técnicas a las instalaciones eléctricas e hidráulicas del edificio, para determinar su capacidad disponible y la requerida para el correcto funcionamiento de las dependencias y los servicios, a fin de programar las acciones de conservación y mantenimiento requeridas.

ARTICULO 42º.- La Dirección de Control Operativo elaborará un plan anual de mantenimiento y conservación del edificio con su correspondiente costeo, el que con la aprobación de las autoridades pertinentes, será incorporado en el Presupuesto Anual.

CAPITULO V

DEL FUNCIONAMIENTO, MANTENIMIENTO y CONSULTA DE LOS ARCHIVOS

ARTÍCULO 43º.- Los Archivos Sectoriales y Centrales de cada Ministerio dependientes del Poder Ejecutivo Provincial, deberán regirse por la normativa establecida en la Ley Nº 5307, Decreto Nº 1417-SCE y Decreto Nº 029-MG-07 (Tablas de Retención). Toda documentación que se encuentre en la normativa antes citada deberá mantenerse en conservación y custodia en los Archivos asignados a cada área en los subsuelos del Centro Cívico.

ARTÍCULO 44º.- Como Anexo Nº III se incorpora al presente la Tabla de Retención Documental en una Tipología Común a todas las Reparticiones dependientes del Poder Ejecutivo Provincial, donde se detalla el tiempo de guarda en cada área y se establece el destino final, asimismo se establece que cada Ministerio deberá elaborar su propia Tabla de Retención Documental la que deberá ser informada al Sistema Provincial de Archivos (SIPAR), para analizar y someter a consideración del Poder Ejecutivo Provincial.

ARTICULO 45º.- Por ninguna causa los Archivos Centrales podrán tener el nombre de Archivo General según lo establece la normativa de la Ley Nº 5307 Capítulo VI Art. 23º, actualmente en vigencia.

CAPITULO VI

DEL FUNCIONAMIENTO Y MANTENIMIENTO DE LOS SISTEMAS INFORMATICOS

ARTICULO 46º.- La instalación de nuevo equipamiento informático deberá ser autorizada por la Coordinación del Gobierno Electrónico quien constatará que el mismo se ajuste a los estándares establecidos por la Dirección Provincial de Informática. No está permitido realizar adaptaciones ni ampliaciones a la estructura de la red ya sea mediante el tendido de cableado o la incorporación de componentes inalámbricos sin la autorización correspondiente. La instalación de equipos servidores deberá realizarse exclusivamente en el espacio reservado para los mismos en el Data Center ubicado en el primer subsuelo.

ARTICULO 47º.- Todos los componentes de software instalado en los equipos del edifico deberán contar con la correspondiente licencia de uso o tratarse de software de libre licenciamiento, quedando bajo responsabilidad del usuario del equipo y del responsable de la repartición la utilización indebida del mismo.

ARTICULO 48º.- El servicio de Internet se otorga con la finalidad que el mismo sea usado exclusivamente para la gestión y tareas que demande la Administración Pública. Las conexiones inapropiadas a Internet pueden dar lugar a que usuarios no autorizados obtengan acceso a las redes internas. Los usuarios autorizados deben utilizar como medio de comunicación el software y el hardware de salida provisto por el Gobierno. No está permitido realizar la descarga de programas, música, videos ni ninguna otra aplicación que infrinja la ley de propiedad intelectual. Está prohibido transmitir por Internet información confidencial, material que viole derechos de autor, material obsceno o información protegida por secreto comercial. Como página de inicio de la sesión del navegador a utilizar para internet deberá configurarse el Sitio Oficial del Gobierno de San Juan, cuya dirección es www.sanjuan.gov.ar

ARTICULO 49º.- No está permitido utilizar el logotipo y nombre del Gobierno Provincial, sistemas, bases de datos, informaciones internas, informes gerenciales, y otras similares en servidores de acceso público o de terceros sin la correspondiente aprobación del responsable de la Repartición correspondiente. Está prohibida la utilización de información en cualquier formato o estructura fuera del ámbito laboral y distinta a la finalidad para la cual fuera conformada sin la correspondiente autorización.

CAPITULO VII

DE LOS AGENTES PUBLICOS

ARTÍCULO 45º.- El personal que cumpla funciones efectivas dentro del edificio Centro Cívico está obligado a procurar un buen clima de trabajo, tanto en su área de acción como en la totalidad del edificio, debiendo reportar inmediatamente a la Secretaría de la Gestión Pública situaciones de violencia laboral en conformidad a lo previsto para la Ley Nº 7939.

ARTICULO 51º.- En caso de violación a lo normado en el presente reglamento será de aplicación el Régimen Disciplinarios previsto por la Ley Nº 3816 o por la normativa que lo remplace en el futuro.

ARTÍCULO 52º.- Es obligación del personal que se encuentre en el Edificio Centro Cívico observar medidas de buen uso, la que estará bajo la supervisión de la Dirección de Control Operativo y/o la Secretaría de la Gestión Pública

ARTICULO 53°.- La disposiciones establecidas en el presente decreto serán de aplicación supletoria para el personal de la Sucursal Banco San Juan instalada en el edificio Centro Cívico.

ARTÍCULO 54º.- Cada área de cocina que posee el edificio será administrada por las dependencias de gobierno que compartan el mismo núcleo, donde obrará personal de maestranza. Será responsabilidad de las respectivas autoridades asignar el personal que mantenga el aseo pertinente de las mismas.

ANEXO II

LEY Nº 7.447.-

LA CÁMARA DE DIPUTADOS DE LA PROVINCIA DE SAN JUAN

SANCIONA CON FUERZA DE L E Y:

ARTÍCULO 1º.- Las personas físicas o jurídicas, que como actividad principal o accesoria se dediquen a almacenar datos o elaborar informes para sí o para terceros sobre la situación comercial o financiera de los ciudadanos, deberán, previamente, estar debidamente inscriptas en el Registro Público de Comercio, reconocer estatutariamente esa finalidad y registrarse en tal carácter en la Dirección de Defensa al Consumidor.-

ARTÍCULO 2º.- Los datos bajo cualquier tipo de guarda o archivos concernientes a los ciudadanos, solamente podrán incorporarse a los registros e informes, de las personas que señala el Artículo 1º, sólo cuando provengan del propio deudor, del acreedor, o de otras fuentes públicas o privadas que estén debidamente autorizadas para emitirlos.-

ARTÍCULO 3º.- Para las personas físicas o jurídicas que señala el Artículo 1º, constituye obligación el conservar por el término de diez (10) años la documentación probatoria de los datos colectados y obtenidos por la información de la entidad pública o privada, del acreedor o del propio deudor, documentación esta que constituye condición indispensable para la registración.-

ARTÍCULO 4º.- Los responsables de la colecta y registro del dato, deberán notificar fehacientemente al interesado, en su domicilio real o legal, y en un término mínimo de diez (10) días anteriores a la fecha del posible uso del informe obtenido, consignando el dato registrado, nombre y domicilio del emisor del dato, la

finalidad que se le dará a la información y toda otra circunstancia que se haya incorporado al registro o banco de datos. La información deberá ser veraz y auténtica, respetándosele al informado su más amplio derecho de defensa en preservación de esta especial garantía constitucional individual.-

ARTÍCULO 5º.- Sin perjuicio de las acciones que constitucional o legalmente le asistan al informado, éste podrá, dentro del plazo anterior ordenado, requerir a los responsables la supresión, corrección o modificación del dato consignado, acreditando fehacientemente los extremos que tornen pertinente su queja.-

ARTÍCULO 6º.- Recibida la petición de modificación, supresión o corrección del dato registrado, los responsables deberán proceder conforme a Ley y notificar al interesado, en el término de setenta y dos (72) horas de recibida la queja, sobre lo evaluado y resuelto.-

ARTÍCULO 7º.- Queda absolutamente prohibido a estos tipos de empresas incorporar datos colectados en mesa de entrada o registraciones del Poder Judicial que no constituyan pronunciamiento jurisdiccionales de los magistrados competentes, o de los registros de matriculados de las personas jurídicas de derecho público no dependiente de los poderes del Estado, ello sin perjuicio de lo establecido en el Artículo 2º.-

ARTÍCULO 8º.- Queda prohibido, asimismo, la incorporación de datos provenientes de oficinas de recaudación o cobro del Poder Ejecutivo Provincial o Municipal, que no provengan de un acto administrativo o certificación de deuda emitido legalmente sin perjuicio de lo establecido en el Artículo 2º.-

ARTÍCULO 9º.- La Corte de Justicia deberá reglamentar en el término de treinta (30) días, a partir de la publicación de la presente norma, lo concerniente al acceso y uso de la información que con carácter meramente administrativo o de información para las partes o letrados se emitan en la órbita de ese Poder del Estado.-

ARTÍCULO 10º.- Todo ciudadano que se crea afectado en su derecho a causa de la registración de datos o producción de informes por parte de las empresas dedicadas a ello, podrá reclamar judicialmente el cese de la situación por procedimientos expeditos o sumarísimos que se sustanciará en idéntica forma que la acción de amparo.

Igual derecho asistirá a aquél que estando correctamente incorporado a las listas de morosos, no fuera inmediatamente excluido, sin necesidad de requerimiento previo, de tal inhabilitación o interdicción en el ejercicio parcial o total de actos de la vida civil, una vez extinguida su condición de deudor.-

ARTÍCULO 11º.- Los responsables que no hubieren cumplido con las exigencias impuestas en los artículos precedentes, o que sin causa razonable acreditable, no hubieren suprimido, corregido o modificado datos erróneamente incorporados a pesar del procedimiento impuesto en los Artículos 5º y 6º, serán solidariamente responsables con el emisor del dato frente al perjuicio objetivo ocasionado.-

ARTÍCULO 12º.- Las empresas que, al momento de la vigencia de esta Ley, hubiesen incorporado a sus registros o base informática datos de ciudadanos para su ulterior uso comercial conforme a su giro, deberán informar fehacientemente a los interesados, sobre los derechos que consagra esta Ley, su extensión y finalidad a los fines previstos en los Artículos 4º; 5º; 6º y 10º, de la presente Ley.-

ARTÍCULO 13º.- El Poder Ejecutivo Provincial reglamentará la presente Ley dentro de los sesenta (60) días de publicada, en lo que sea pertinente, sin perjuicio de las partes operativas de aplicación inmediata.-

ARTÍCULO 14º.- Comuníquese al Poder Ejecutivo.-

Sala de Sesiones de la Cámara de Diputados, a los veinte días del mes de noviembre del año dos mil tres.-

ANEXO III

El contenido de los cursos dictados es el contempló los siguientes temas:

- Common Language Runtime (CLR)
- Microsoft Intermediate Language (MSIL)
- Metadatos
- Librería de clase base (BCL)
- Common Type System (CTS)
- Common Language Specification (CLS)
- Características de C#
- Concepto de preprocesador
- Directivas de preprocesado
- Sintaxis
- Manejo de Variables
- Manejo de: clases, Objetos, Herencia, métodos virtuales
- Funciones parámetros, Métodos, Constructores, Destructores
- Sintaxis general de uso del compilador
- Opciones de compilación
- Familiarización con los conceptos del framework .net compacto para dispositivos móviles
- Instalación y configuración de entorno de desarrollo
- Desarrollo de interfaz
- Input del usuario
- Servicios Web XML
- SQL Server CE (versión de SQL Server para dispositivos móviles)

- Seguridad en SQL Server CE
- Construcción de un cliente simple
- Administrar datos y el acceso a los mismos
- Acceso remoto a la información
- Crear paginas con "Mobile Web Controls" (Controles web para dispositivos móviles)
- Sincronizar datos desde dispositivos
- Seguridad para el entorno móvil
- Debug y testeo de aplicaciones móviles
- MMIT (Microsoft Mobile Internet Toolkit)

ANEXO IV

LEY 25326 HÁBEAS DATA

Protección de los datos personales. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección sanc. 04/10/2000; promul. 30/10/2000; publ. 02/11/2000

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de ley:

LEY DE PROTECCIÓN DE LOS DATOS PERSONALES

CAPÍTULO I:

DISPOSICIONES GENERALES

Art. 1.– (Objeto). La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el art. 43 Ver Texto , párr. 3 de la Constitución Nacional.

Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.

En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas.

Art. 2.– (Definiciones). A los fines de la presente ley se entiende por:

- Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

- Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

- Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

- Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

- Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

- Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

- Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

- Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

- Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

CAPÍTULO II:

PRINCIPIOS GENERALES RELATIVOS A LA PROTECCIÓN DE DATOS

Art. 3.– (Archivos de datos - Licitud). La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los

principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia.

Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública.

Art. 4.– (Calidad de los datos).

1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.

3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.

5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el art. 16 Ver Texto de la presente ley.

6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

Art. 5.– (Consentimiento).

1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el art. 6 Ver Texto de la presente ley.

2. No será necesario el consentimiento cuando:

a) Los datos se obtengan de fuentes de acceso público irrestricto;

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;

c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;

d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;

e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del art. 39 Ver Texto de la ley 21526.

Art. 6.– (Información). Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:

a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;

b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;

c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;

d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;

e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

Art. 7.– (Categoría de datos).

1. Ninguna persona puede ser obligada a proporcionar datos sensibles.

2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.

4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.

Art. 8.– (Datos relativos a la salud). Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional.

Art. 9.– (Seguridad de los datos).

1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

Art. 10.– (Deber de confidencialidad).

1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.

2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

Art. 11.– (Cesión).

1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.

2. El consentimiento para la cesión es revocable.

3. El consentimiento no es exigido cuando:

a) Así lo disponga una ley;

b) En los supuestos previstos en el art. 5 Ver Texto inc. 2;

c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias;

d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados;

e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.

4. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.

Art. 12.– (Transferencia internacional).

1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.

2. La prohibición no regirá en los siguientes supuestos:

a) Colaboración judicial internacional;

b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inc.

e) del artículo anterior;

c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;

d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;

e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

CAPÍTULO III:

DERECHOS DE LOS TITULARES DE DATOS

Art. 13.– (Derecho de Información). Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita.

Art. 14.– (Derecho de acceso).

1. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.

2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente.

Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley.

3. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.

4. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales.

Art. 15.– (Contenido de la información).

1. La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen.

2. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.

3. La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.

Art. 16.– (Derecho de rectificación, actualización o supresión).

1. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.

2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.

3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley.

4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.

5. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.

6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.

7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos.

Art. 17.– (Excepciones).

1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.

2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado.

3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa.

Art. 18.– (Comisiones legislativas). Las Comisiones de Defensa Nacional y la Comisión Bicameral de Fiscalización de los Órganos y Actividades de Seguridad Interior e Inteligencia del Congreso de la Nación y la Comisión de Seguridad Interior de la Cámara de Diputados de la Nación, o las que las sustituyan, tendrán acceso a los archivos o bancos de datos referidos en el art. 23 Ver Texto inc. 2 por razones

fundadas y en aquellos aspectos que constituyan materia de competencia de tales Comisiones.

Art. 19.– (Gratuidad). La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros públicos o privados se efectuará sin cargo alguno para el interesado.

Art. 20.– (Impugnación de valoraciones personales). 1. Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado.

2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos.

CAPÍTULO IV:

USUARIOS Y RESPONSABLES DE ARCHIVOS, REGISTROS Y BANCOS DE DATOS

Art. 21.– (Registro de archivos de datos. Inscripción).

1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el registro que al efecto habilite el organismo de control.

2. El registro de archivos de datos debe comprender como mínimo la siguiente información:

a) Nombre y domicilio del responsable;

b) Características y finalidad del archivo;

c) Naturaleza de los datos personales contenidos en cada archivo;

d) Forma de recolección y actualización de datos;

e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;

f) Modo de interrelacionar la información registrada;

g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;

h) Tiempo de conservación de los datos;

i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

3. Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro.

El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en el cap. VI de la presente ley.

Art. 22.– (Archivos, registros o bancos de datos públicos).

1. Las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos deben hacerse por medio de disposición general publicada en el Boletín Oficial de la Nación o diario oficial.

2. Las disposiciones respectivas, deben indicar:

a) Características y finalidad del archivo;

b) Personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas;

c) Procedimiento de obtención y actualización de los datos;

d) Estructura básica del archivo, informatizado o no, y la descripción de la naturaleza de los datos personales que contendrán;

e) Las cesiones, transferencias o interconexiones previstas;

f) Órganos responsables del archivo, precisando dependencia jerárquica en su caso;

g) Las oficinas ante las que se pudiesen efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación o supresión.

3. En las disposiciones que se dicten para la supresión de los registros informatizados se establecerá el destino de los mismos o las medidas que se adopten para su destrucción.

Art. 23.– (Supuestos especiales).

1. Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.

2. El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad.

3. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

Art. 24.– (Archivos, registros o bancos de datos privados). Los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto en el art. 21 Ver Texto .

Art. 25.– (Prestación de servicios informatizados de datos personales).

1. Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.

2. Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta

de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.

Art. 26.– (Prestación de servicios de información crediticia).

1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés.

3. A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión.

4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hace constar dicho hecho.

5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

Art. 27.– (Archivos, registros o bancos de datos con fines de publicidad).

1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.

2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.

3. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo.

Art. 28.– (Archivos, registros o bancos de datos relativos a encuestas).

1. Las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a ley 17622 Ver Texto , trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable.

2. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna.

CAPÍTULO V:

CONTROL

Art. 29.– (Órgano de control).

1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones:

a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza;

b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley;

c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos;

d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá

solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley;

e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados;

f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia;

g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley;

h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el registro creado por esta ley.

2. (Observado por decreto 995/2000, art. 1 Ver Texto). El órgano de control gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación.

3. (Observado por decreto 995/2000, art. 1 Ver Texto). El órgano de control será dirigido y administrado por un director designado por el término de cuatro (4) años, por el Poder Ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia.

El director tendrá dedicación exclusiva en su función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones.

Art. 30.– (Códigos de conducta). 1. Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar

y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley.

2. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia.

CAPÍTULO VI:

SANCIONES

Art. 31.– (Sanciones administrativas).

1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.) a cien mil pesos ($ 100.000.), clausura o cancelación del archivo, registro o banco de datos.

2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.

Art. 32.– (Sanciones penales).

1. Incorpórase como art. 117 bis Ver Texto del Código Penal, el siguiente:

1. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.

2. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.

3. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.

4. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena.

2. Incorpórase como art. 157 bis Ver Texto del Código Penal el siguiente: “Será reprimido con la pena de prisión de un mes a dos años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años”.

CAPÍTULO VII:

ACCIÓN DE PROTECCIÓN DE LOS DATOS PERSONALES

Art. 33.– (Procedencia).

1. La acción de protección de los datos personales o de hábeas data procederá:

a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;

b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.

Art. 34.– (Legitimación activa). La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado.

Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto.

En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo.

Art. 35.– (Legitimación pasiva). La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes.

Art. 36.– (Competencia). Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor.

Procederá la competencia federal:

a) cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y

b) cuando los archivos de datos se encuentren interconectados en redes interjurisdicciones (Sic B.O.), nacionales o internacionales.

Art. 37.– (Procedimiento aplicable). La acción de hábeas data tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo común y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo.

Art. 38.– (Requisitos de la demanda).

1. La demanda deberá interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del archivo, registro o banco de datos y, en su caso, el nombre del responsable o usuario del mismo.

En el caso de los archivos, registros o bancos públicos, se procurará establecer el organismo estatal del cual dependen.

2. El accionante deberá alegar las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley.

3. El afectado podrá solicitar que mientras dure el procedimiento, el registro o banco de datos asiente que la información cuestionada está sometida a un proceso judicial.

4. El juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate.

5. A los efectos de requerir información al archivo, registro o banco de datos involucrado, el criterio judicial de apreciación de las circunstancias requeridas en los ptos. 1 y 2 debe ser amplio.

Art. 39.– (Trámite).

1. Admitida la acción el juez requerirá al archivo, registro o banco de datos la remisión de la información concerniente al accionante. Podrá asimismo solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente.

2. El plazo para contestar el informe no podrá ser mayor de cinco días hábiles, el que podrá ser ampliado prudencialmente por el juez.

Art. 40.– (Confidencialidad de la información).

1. Los registros, archivos o bancos de datos privados no podrán alegar la confidencialidad de la información que se les requiere salvo el caso en que se afecten las fuentes de información periodística.

2. Cuando un archivo, registro o banco de datos público se oponga a la remisión del informe solicitado con invocación de las excepciones al derecho de acceso, rectificación o supresión, autorizadas por la presente ley o por una ley específica; deberá acreditar los extremos que hacen aplicable la excepción legal. En tales casos, el juez podrá tomar conocimiento personal y directo de los datos solicitados asegurando el mantenimiento de su confidencialidad.

Art. 41.– (Contestación del informe). Al contestar el informe, el archivo, registro o banco de datos deberá expresar las razones por las cuales incluyó la información cuestionada y aquellas por las que no evacuó el pedido efectuado por el

interesado, de conformidad a lo establecido en los arts. 13 Ver Texto a 15 Ver Texto de la ley.

Art. 42.– (Ampliación de la demanda). Contestado el informe, el actor podrá, en el término de tres días, ampliar el objeto de la demanda solicitando la supresión, rectificación, confidencialidad o actualización de sus datos personales, en los casos que resulte procedente a tenor de la presente ley, ofreciendo en el mismo acto la prueba pertinente. De esta presentación se dará traslado al demandado por el término de tres días.

Art. 43.– (Sentencia).

1. Vencido el plazo para la contestación del informe o contestado el mismo, y en el supuesto del art. 42 Ver Texto , luego de contestada la ampliación, y habiendo sido producida en su caso la prueba, el juez dictará sentencia.

2. En el caso de estimarse procedente la acción, se especificará si la información debe ser suprimida, rectificada, actualizada o declarada confidencial, estableciendo un plazo para su cumplimiento.

3. El rechazo de la acción no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir el demandante.

4. En cualquier caso, la sentencia deberá ser comunicada al organismo de control, que deberá llevar un registro al efecto.

Art. 44.– (Ámbito de aplicación). Las normas de la presente ley contenidas en los caps. I, II, III y IV, y art. 32 Ver Texto son de orden público y de aplicación en lo pertinente en todo el territorio nacional.

Se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional.

La jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional.

Art. 45.– El Poder Ejecutivo nacional deberá reglamentar la presente ley y establecer el organismo de control dentro de los ciento ochenta días de su promulgación.

Art. 46.– (Disposiciones transitorias). (*) Los archivos, registros, bases o bancos de datos destinados a proporcionar informes, existentes al momento de la sanción de la presente ley, deberán inscribirse en el registro que se habilite conforme a lo dispuesto en el art. 21 Ver Texto y adecuarse a lo que dispone el presente régimen dentro del plazo que al efecto establezca la reglamentación.

(*) El art. 2 Ver Texto del decreto 1558/2001 establece: “Establécese en ciento ochenta (180) días el plazo previsto en el art. 46 Ver Texto de la ley 25326”.

Art. 47.– (Incorporado por ley 26343, art. 1 Ver Texto) Los bancos de datos destinados a prestar servicios de información crediticia deberán eliminar y omitir el asiento en el futuro de todo dato referido a obligaciones y calificaciones asociadas de las personas físicas y jurídicas cuyas obligaciones comerciales se hubieran constituido en mora, o cuyas obligaciones financieras hubieran sido clasificadas con categoría 2, 3, 4 ó 5, según normativas del Banco Central de la República Argentina, en ambos casos durante el período comprendido entre el 1º de enero del año 2000 y el 10 de diciembre de 2003, siempre y cuando esas deudas hubieran sido canceladas o regularizadas al momento de entrada en vigencia de la presente ley o lo sean dentro de los 180 días posteriores a la misma. La suscripción de un plan de pagos por parte del deudor, o la homologación del acuerdo preventivo o del acuerdo preventivo extrajudicial importará la regularización de la deuda, a los fines de esta ley.

El Banco Central de la República Argentina establecerá los mecanismos que deben cumplir las Entidades Financieras para informar a dicho organismo los datos necesarios para la determinación de los casos encuadrados. Una vez obtenida dicha información, el Banco Central de la República Argentina implementará las medidas necesarias para asegurar que todos aquellos que consultan los datos de su Central de Deudores sean informados de la procedencia e implicancias de lo aquí dispuesto.

Toda persona que considerase que sus obligaciones canceladas o regularizadas están incluidas en lo prescripto en el presente artículo puede hacer uso de los derechos de acceso, rectificación y actualización en relación con lo establecido.

Sin perjuicio de lo expuesto en los párrafos precedentes, el acreedor debe comunicar a todo archivo, registro o banco de datos al que hubiera cedido datos referentes al incumplimiento de la obligación original, su cancelación o regularización.

Art. 47.- (Observado por decreto 995/2000, art. 2 Ver Texto). Los bancos de datos prestadores de servicios de información crediticia deberán suprimir, o en su caso, omitir asentar, todo dato referido al incumplimiento o mora en el pago de una obligación, si ésta hubiere sido cancelada al momento de la entrada en vigencia de la presente ley.

Art. 48.– Comuníquese, etc.

Pascual - Genoud - Aramburu – Pontaquarto

LEY Nº 7.447.-

LA CÁMARA DE DIPUTADOS DE LA PROVINCIA DE SAN JUAN

SANCIONA CON FUERZA DE L E Y :

ARTÍCULO 1º.- Las personas físicas o jurídicas, que como actividad principal o accesoria se dediquen a almacenar datos o elaborar informes para sí o para terceros sobre la situación comercial o financiera de los ciudadanos, deberán, previamente, estar debidamente inscriptas en el Registro Público de Comercio, reconocer estatutariamente esa finalidad y registrarse en tal carácter en la Dirección de Defensa al Consumidor.-

ARTÍCULO 2º.- Los datos bajo cualquier tipo de guarda o archivos concernientes a los ciudadanos, solamente podrán incorporarse a los registros e informes, de las personas que señala el Artículo 1º, sólo cuando provengan del

propio deudor, del acreedor, o de otras fuentes públicas o privadas que estén debidamente autorizadas para emitirlos.-

ARTÍCULO 3º.- Para las personas físicas o jurídicas que señala el Artículo 1º, constituye obligación el conservar por el término de diez (10) años la documentación probatoria de los datos colectados y obtenidos por la información de la entidad pública o privada, del acreedor o del propio deudor, documentación esta que constituye condición indispensable para la registración.-

ARTÍCULO 4º.- Los responsables de la colecta y registro del dato, deberán notificar fehacientemente al interesado, en su domicilio real o legal, y en un término mínimo de diez (10) días anteriores a la fecha del posible uso del informe obtenido, consignando el dato registrado, nombre y domicilio del emisor del dato, la finalidad que se le dará a la información y toda otra circunstancia que se haya incorporado al registro o banco de datos. La información deberá ser veraz y auténtica, respetándosele al informado su más amplio derecho de defensa en preservación de esta especial garantía constitucional individual.-

ARTÍCULO 5º.- Sin perjuicio de las acciones que constitucional o legalmente le asistan al informado, éste podrá, dentro del plazo anterior ordenado, requerir a los responsables la supresión, corrección o modificación del dato consignado, acreditando fehacientemente los extremos que tornen pertinente su queja.-

ARTÍCULO 6º.- Recibida la petición de modificación, supresión o corrección del dato registrado, los responsables deberán proceder conforme a Ley y notificar al interesado, en el término de setenta y dos (72) horas de recibida la queja, sobre lo evaluado y resuelto.-

ARTÍCULO 7º.- Queda absolutamente prohibido a estos tipos de empresas incorporar datos colectados en mesa de entrada o registraciones del Poder Judicial que no constituyan pronunciamiento jurisdiccionales de los magistrados competentes, o de los registros de matriculados de las personas jurídicas de derecho público no dependiente de los poderes del Estado, ello sin perjuicio de lo establecido en el Artículo 2º.-

ARTÍCULO 8º.- Queda prohibido, asimismo, la incorporación de datos provenientes de oficinas de recaudación o cobro del Poder Ejecutivo Provincial o Municipal, que no provengan de un acto administrativo o certificación de deuda emitido legalmente sin perjuicio de lo establecido en el Artículo 2º.-

ARTÍCULO 9º.- La Corte de Justicia deberá reglamentar en el término de treinta (30) días, a partir de la publicación de la presente norma, lo concerniente al acceso y uso de la información que con carácter meramente administrativo o de información para las partes o letrados se emitan en la órbita de ese Poder del Estado.-

ARTÍCULO 10º.- Todo ciudadano que se crea afectado en su derecho a causa de la registración de datos o producción de informes por parte de las empresas dedicadas a ello, podrá reclamar judicialmente el cese de la situación por procedimientos expeditos o sumarísimos que se sustanciará en idéntica forma que la acción de amparo. Igual derecho asistirá a aquél que estando correctamente incorporado a las listas de morosos, no fuera inmediatamente excluido, sin necesidad de requerimiento previo, de tal inhabilitación o interdicción en el ejercicio parcial o total de actos de la vida civil, una vez extinguida su condición de deudor.-

ARTÍCULO 11º.- Los responsables que no hubieren cumplido con las exigencias impuestas en los artículos precedentes, o que sin causa razonable acreditable, no hubieren suprimido, corregido o modificado datos erróneamente incorporados a pesar del procedimiento impuesto en los Artículos 5º y 6º, serán solidariamente responsables con el emisor del dato frente al perjuicio objetivo ocasionado.-

ARTÍCULO 12º.- Las empresas que, al momento de la vigencia de esta Ley, hubiesen incorporado a sus registros o base informática datos de ciudadanos para su ulterior uso comercial conforme a su giro, deberán informar fehacientemente a los interesados, sobre los derechos que consagra esta Ley, su extensión y finalidad a los fines previstos en los Artículos 4º; 5º; 6º y 10º, de la presente Ley.-

ARTÍCULO 13º.- El Poder Ejecutivo Provincial reglamentará la presente Ley dentro de los sesenta (60) días de publicada, en lo que sea pertinente, sin perjuicio de las partes operativas de aplicación inmediata.-

ARTÍCULO 14º.- Comuníquese al Poder Ejecutivo.-

Sala de Sesiones de la Cámara de Diputados, a los veinte días del mes de noviembre del año dos mil tres.-

ANEXO V

Requerimientos para el proyecto de implantación de una solución de antivirus.

Descripción

Se prevé ampliar la solución de antivirus implementada a nivel de Gobierno de la provincia de San Juan.

El objetivo primario es llevar a cabo la contratación del servicio integral de diseño e implementación de la citada ampliación. En forma conjunta llevar a cabo la capacitación del personal de Gobierno designado a fin de que logre el conocimiento necesario para operar la solución en forma autónoma..

Condiciones

Las siguientes condiciones se deben considerar a la hora de proponer la solución:

Posibilidad de ampliación del paquete de licencias en forma dinámica. Con un acuerdo previo con el proveedor.

Soporte a distribuciones LINUX.

Contar con versiones para: Desktop, File Server, Firewall/Gateway, Concentrador de VPN, Virtualización y Base de Datos.

La autentificación y seguridad definida deberá integrarse con Microsoft Active Directory.

Soporte post-instalación.

Solución de consola centralizada para la administración integral de la solución.

Dos (2) meses como tiempo propuesto para la implementación completa.

Entregables

La propuesta de solución debe agrupar los siguientes productos:

Alcance.

Objetivos.

Diseño de la solución. A nivel de hardware, software y servicios.

Plan de implementación.

Implementación y despliegue.

Plan de Operación.

Ejecución de los protocolos de prueba y presentación de los resultados de las mismas.

Nota: Respecto al hardware, solo se requiere efectuar el diseño de la infraestructura de hardware adecuada para soportar la propuesta de solución. No siendo necesaria la provisión del mismo.

Volumen de Licenciamiento.

Se estima ampliar el número de licencias en dos mil cien (2.100). Esta cantidad se distribuye entre desktops y FileServer.

Estrategia de Despliegue propuesta

Se propone el siguiente conjunto de actividades de despliegue a desarrollar a efecto de garantizar la puesta en marcha de la solución de antivirus:

Instalación de los componentes servidores y la consola de administración centralizada.

Implementación de la arquitectura de administración de la consola.

Implementación Arquitectura y distribución de clientes a 50 usuarios “on- site” en forma conjunta (proveedor y cliente) y el resto a cargo del cliente asistido por el proveedor.

Capacitación de tipo “on –site” (Operación y Mantenimiento de la solución a alto nivel).

Soporte Post-Implementación (Remoto) hasta 30 días hábiles después de cerrada la última actividad del plan de trabajo.

Capacitación

El objetivo principal es transmitir al personal de Gobierno el conocimiento en el uso de las herramientas tecnológicas para la administración y gestión diaria de la plataforma de seguridad a implementar. Para ello se propone la modalidad On–Job-Training. Este entrenamiento estará a cargo del proveedor, siendo el destinatario de la misma los agentes destinados a tal fin. De esta forma se persigue conformar un equipo de trabajo, con la autonomía suficiente, para operar el servicio en forma integral.

Servicio de Soporte Técnico

Durante el período del Servicio de Mantenimiento de 30 días posteriores a la puesta en marcha de la solución, se brindará soporte remoto y/o telefónico.

Las consultas sobre el funcionamiento, operación, alcances del producto y anomalías menores, que no afectan en forma crítica el normal desempeño del producto o servicio, serán tratadas mediante correspondencia vía e-mail

En presencia de fallas de mayor importancia, que limiten el funcionamiento o la operación de dicho producto, el contacto con el Centro de Servicios al Cliente será a través de comunicaciones telefónicas.