CONSEJO FEDERAL DE INVERSIONES

Provincia de San Juan

Sistema Unificado de Gestión Documental

Informe FINAL

Octubre 2017

Autor: ***Mag. Horacio D. SANCHEZ***

Índice Temático

Definición del Contexto

Realidad Político/Económica actual de la Gestión de TI

A partir de los nuevos proyectos encarados desde fines del año 2015 en las áreas Informáticas del Gobierno, se inició una importante transformación en todos los ámbitos ministeriales. Particularmente, en Tecnologías de la Información y las Comunicaciones (TICs), donde se adoptó un cambio profundo en la gestión y administración técnica de las mismas. Se definió un enfoque integrador, de centralización en la prestación de los servicios TI (Tecnologías de la Información). Complementariamente, se definió el concepto de “transversalidad” en cuanto a la adopción de tecnologías, estándares, soluciones, servicios y sistemas. Se avanzó fuertemente también en la coordinación de los equipos de trabajos relacionados con las TICs en todo el ámbito del Poder Ejecutivo provincial. Se inició la transformación de puestos de trabajo y áreas de prestación de servicio, a fin de potenciar sus capacidades de operación y rendimiento. Se emprendieron cambios profundos en la reestructuración de los espacios de trabajo asociados a la actividad informática.

En lo referente a las áreas de sistemas de software, se comenzó a trabajar en la consolidación de los equipos de desarrollo. Las nuevas políticas apuntaron a conformar equipos propios de Gobierno, que sean capaces de emprender todas las etapas del ciclo de vida de desarrollo de sistemas. Estos equipos, inicialmente se conformarán en forma mixta entre los agentes de la administración pública e integrantes de equipos de consultores externos. Estos últimos trabajaron inicialmente en el desarrollo de las soluciones contratadas en conjunto con los equipos de sistemas de Gobierno.

Otra política central que se definió fue la provisión de Servicios TI en forma centralizada, especialmente desde las áreas técnicas de la Secretaría de la Gestión Pública (SGP) dependiente del Ministerio de Hacienda y Finanzas del Gobierno de la Provincia de San Juan. Esto decantó en la conformación de unidades técnicas especializadas, capaces de ofrecer la provisión de servicios integrales y soporte a todo el Poder Ejecutivo Provincial desde la (SGP).

Estas nuevas políticas, acompañadas de importantes transformaciones, produjeron cambios sustanciales en el diseño de los Servicios TI asociados. A lo

largo del desarrollo de esta consultoría, se trabajó colaborativamente con autoridades políticas y técnicas de la SGP en la determinación y definición de nuevos requerimientos y objetivos relacionados con los temas asociados a la presenta consultoría.

Ejes de Acción

La transformación mencionada, iniciada desde la SGP afecta en todos los ejes a Sistemas, Infraestructura y Servicios TI relacionados.

Ahora bien, debido a los cambios a los que se hace referencia, se presentaron demoras en la definición de políticas y concreción de determinados hitos a niveles macros respecto de políticas globales. En un principio se pudieron traducir en demoras a la hora de alcanzar ciertos objetivos específicos. Posteriormente, una vez logrados, se aceleraron los plazos de concreción de los siguientes. Lo mencionado fue producto de las mejoras en la organización e integración de las nuevas áreas relacionadas. Los beneficios impactaron también en los diversos procesos con la conformación de equipos de trabajos más numerosos y de mayor especialización. Se espera, que una vez que logren desarrollarse y adecuarse, permitirán elevar los niveles de producción y rendimiento.

Esta consultoría trabajó sobre tres ejes básicos como fueron: Servicio de Directorio, Soporte al Sistema de Gestión Documental y la Gestión de Infraestructura TI.

El esquema definido para la presente consultoría estaba centrado en el apoyo al Sistema de Gestión Documental. Debido a los cambios mencionados, encarados por la SGP en lo referente al soporte específico al SIGED se decidió, en común acuerdo, darle mayor énfasis al eje de acción asociado al soporte de la Infraestructura TI relacionada. Es decir, dedicarle mayores esfuerzos a consolidar y fortalecer la infraestructura asociada al SIGED. De esta forma, al tratarse de un sistema que se desplegaría en un entorno de Sistemas integrados, lo que pudiese avanzarse e implementarse en este ámbito, beneficiaría a los restantes sistemas y al área de sistemas en su conjunto.

Así, desde esta consultoría. Se elaboró una propuesta de un modelo de monitoreo y gestión de Infraestructura TI a fin de dar soporte al SIGED, y consecuentemente a la infraestructura asociada a los Sistemas Integrados.

El modelo propuesto, también es factible de ser aplicado a otros ámbitos como pueden ser la gestión de redes, gestión de entornos de consolidación y virtualización, gestión de aprovisionamiento de Servicios TI, por nombrar los más relevantes. Por lo cual se redefinieron los términos de referencia de la presente consultoría a fin de complementar de una forma más óptima el ambicioso proyecto central que lleva cabo la Secretaría de la Gestión Pública.

Equipo de Trabajo y Agradecimiento

Esta consultoría fue desarrollada en conjunto con el Lic. *Daniel GALLARDO*, quien conformó el equipo de trabajo como Consultor.

En forma complementaria, se trabajó con personal de la Secretaría de la Gestión Pública dependiente del Ministerio de Hacienda y Finanzas del Gobierno de San Juan. Con todos ellos estamos enormemente agradecidos, por permitirnos lograr en conjunto, los objetivos de la presente consultoría.

Un agradecimiento particular al personal del Consejo Federal de Inversiones por su colaboración y excelente trato.

Y expresamos nuestra gratitud y reconocimiento al Lic. Andrés RUPCIC, Sec. de la Gestión Pública de la Prov. de San Juan, quien fue el impulsor y principal apoyo que tuvimos para la realización de este trabajo.

Servicio de Directorio

Escenario Actual / Actualidad del Servicio

En el ámbito del Poder Ejecutivo de la Provincia de San Juan, existen numerosas implementaciones de Servicios de Directorio. Estas implementaciones, se han desarrollado en forma paralela en diversos ámbitos, respondiendo a distintos requerimientos de diseño, y objetivos organizacionales. Naturalmente, se ha registrado un crecimiento y evolución en cierta forma anárquica. La complejidad y necesidades del día a día; sumado a la falta de una política integradora conlleva a que las distintas instancias desplegadas carezcan de un diseño refinado. Sin poseer una cohesión lógica acorde a las mejores prácticas. Lo anterior enfocado a servicios de nivel corporativo como debería corresponder a un entorno gubernamental integrado.

Luego de efectuar un primer relevamiento, se identifican claramente dos implementaciones del servicio que deberían ser consideradas como la base sobre la cual crecer. Complementariamente, debería centrarse en esta base para iniciar un proceso de rediseño futuro. Esto último se plantea sobre la experiencia de este equipo de consultoría en relación con trabajos anteriores en ámbitos de Gobierno.

Las dos implementaciones son la asociada al dominio “sanjuan.gob” (perteneciente al Ministerio de Hacienda) y el dominio “DOTECME” (perteneciente al Ministerio de Educación).

La implementación asociada al dominio “sanjuan.gob” es la más evolucionada en términos de diseño para escalar en ambas dimensiones. Posee una implementación física robusta de componentes servidores, y con personal técnico con conocimientos avanzados en la administración de la misma. Esta instancia está administrada principalmente por un equipo técnico dependiente de la Secretaría de la Gestión Pública. La infraestructura TI sobre la cual opera es tecnología de gestión unificada de recursos de computo de PureFlex System de IBM. Lo anterior consolidando sobre VMware y con la implementación de una solución de HA en tiempo real.

El servicio se gestiona bajo la modalidad de administración centralizada, pero de operación descentralizada. Lo anterior, refiere a que cualquier unidad organizacional (Ministerio, Secretaría, Dirección, etc.) que integra el Servicio de Directorio puede administrar su red lógica y objetos asociados, al nivel granular que lo desee y con la autonomía suficiente. Lo anterior será posible, siempre y cuando posea la capacidad técnica y operativa de realizarlo. De lo contrario, puede contar son el soporte y gestión centralizada del personal de la SGP.

En la Figura 9, más adelante en el punto “Diseño Lógico Adoptado”, se presenta la estructura en cuanto a las Unidades Organizativas. Aquí se visualiza claramente la implementación del modelo de administración y delegación de administración acorde al diseño que se presenta más adelante en el punto “Diseño actual del Servicio”.

Es claro ver como cada una de las organizaciones (direcciones, secretarías, etc.) se van estructurando para conformar el árbol de administración de objetos del directorio. Y complementariamente se va constituyendo la jerarquía que representará la estructura del directorio de Gobierno.

Nota: *Se empleó la herramienta ADTD (Active Directory Topology Diagrammer) para la realizar una instantánea de la configuración actual del Servicio de Directorio “sanjuan.gob”. Esta herramienta es aconsejable, ya que realiza la extracción de la información directamente desde los controladores de dominio, generando automáticamente salidas gráficas en formato de Microsoft Visio. Es importante, y aconsejable, que la misma sea incorporada a la gestión del Servicio.*

Configuración lógica actual del Servicio de Directorio

A continuación, se presenta la configuración lógica actual del servicio de directorio correspondiente al dominio “sanjuan.gob”.

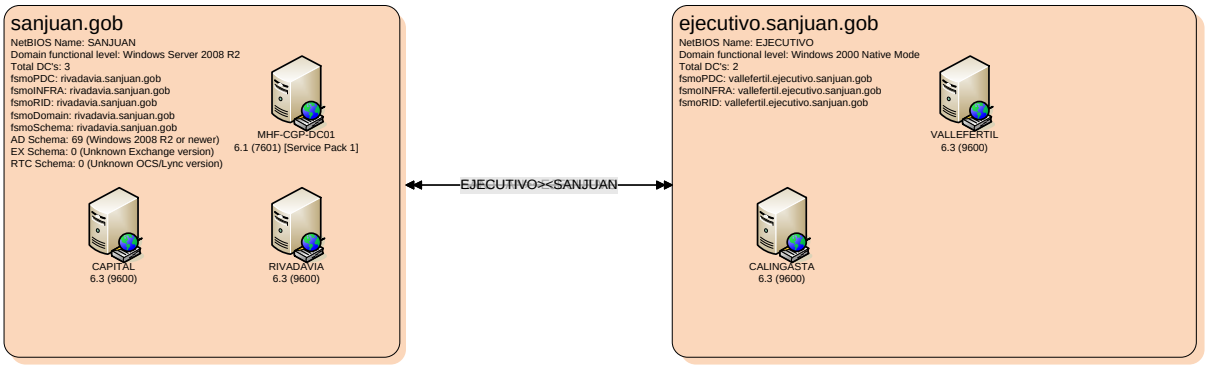


Figura 1 – Distribución de Roles FSMO a nivel de Bosque y Dominio

En la Figura 1 se visualiza la distribución de los roles tanto a nivel de Bosque como de los Dominios.

Si bien esta estructura no está del todo consolidada, uno de los avances aportados desde esta consultoría, es fortalecer el diseño propuesto.

Para el dominio raíz del bosque "*sanjuan.gob*", el DC Rivadavia es el asignado para operar los tres roles a nivel de dominio como son el Maestro de Operaciones de Infraestructura, de Identificadores Relativos (RID) y el emulador de Controlador Primario de Dominio (PDC). Conjuntamente tiene asignados también los dos roles de bosque como son el de Operación del Esquema y el de Nombres de Dominio.

Es decir que en el DC Rivadavia están centralizados los 5 roles naturales de una raíz de bosque.

Complementariamente, para el dominio hijo "*ejecutivo.sanjuan.gob*" se han implementado los tres (3) roles a nivel de dominio en el DC "*vallefertil.ejecutivo.sanjuan.gob*".

Es oportuno aclarar la presencia del Controlador de Dominio "MHF-CGP-DC01", el cual tiene la particularidad de ser un Controlador de Solo Lectura (RODC – *Read Only Domain Controler*, por sus siglas en Ingles).

La existencia de este tipo de Controladores de Dominio permite la autonomía en la operación por parte de ciertas áreas de la organización. Lo anterior, analizado

desde un punto de vista de la disponibilidad del servicio respecto a la ubicación física de los clientes que lo consumen. Ver la Figura 8 más adelante.

La Contaduría General de la Provincia, quien solicitó la creación de esta instancia particular, posee el requerimiento de alta disponibilidad del servicio. Se procedió a la creación de este Controlador, para satisfacer el requerimiento puntual, y fundamentalmente porque no afecta al diseño original de centralización de la administración del dominio. Este requerimiento puntual será estudiado detalladamente más adelante, cuando se defina la nueva topología física a implementarse, y el diseño de la disponibilidad global del Servicio.

La implementación de Controladores de Domino de solo lectura son recomendables en la fase de implementación de nuevos Sitios. En este momento, desde el punto de vista de la presente consultoría, es bueno realizar la experiencia del despliegue de este controlador. La misma servirá de una buena experiencia para el equipo de gestión y administración del servicio.

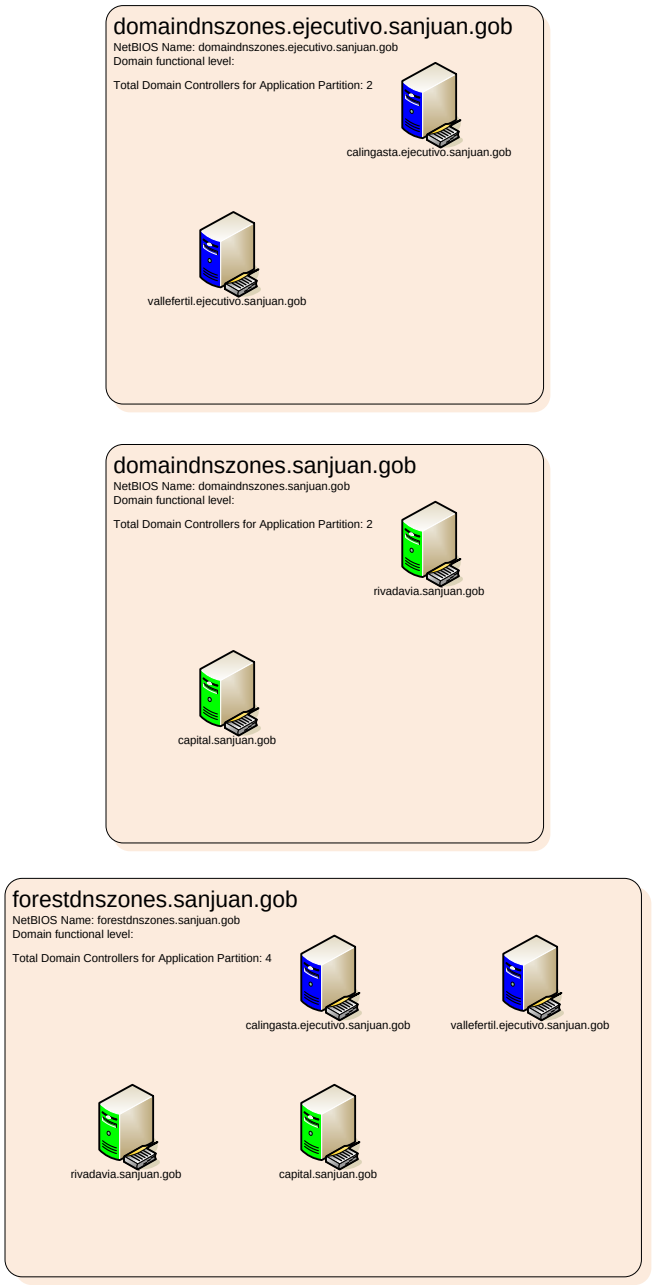


Figura 2 – Configuración de Zonas DNS

La implementación actual del Servicio de DNS relevado es el exclusivo asociado a la operación del servicio de Directorio. Es bueno aclarar que Active Directory implementa de forma nativa el servicio de DNS a nivel de bosque. Sería recomendable realizar un estudio de mayor profundidad respecto al diseño e implementación de la infraestructura DNS asociada a la operación de la red de Gobierno. Lo anterior pensando en integrar la prestación del servicio a nivel de intranet/extranet e internet en forma global a Gobierno.

Actualmente, se encuentran operativos diversos Servicios DNS en el ámbito de la red de Gobierno. Estos Servicios resuelven distintos ámbitos, asociados a la segmentación de la red física. Por lo cual es importante llevar a cabo un análisis profundo de integración y despliegue de una solución integrada. Este nuevo diseño, puede ser un trabajo central a realizarse en una futura consultoría.

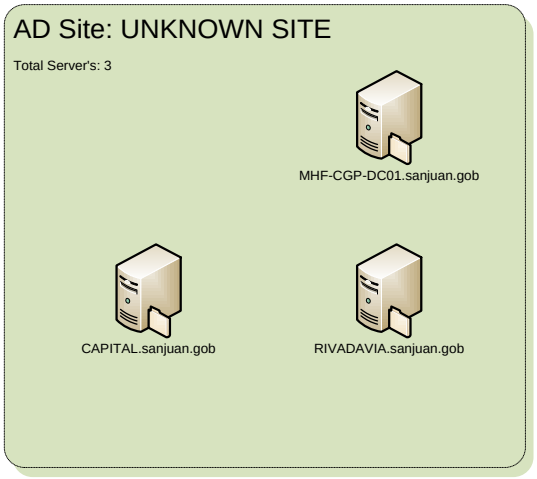


Figura 3 - Configuración de Sitios – Dominio “sanjuan.gob”

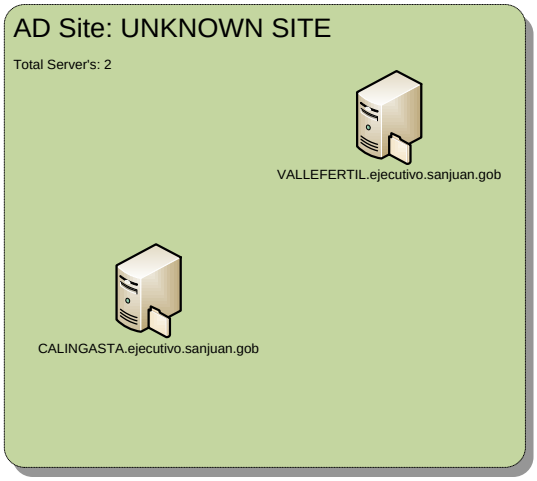


Figura 4 - Configuración de Sitios – Dominio “ejecutivo.sanjuan.gob”

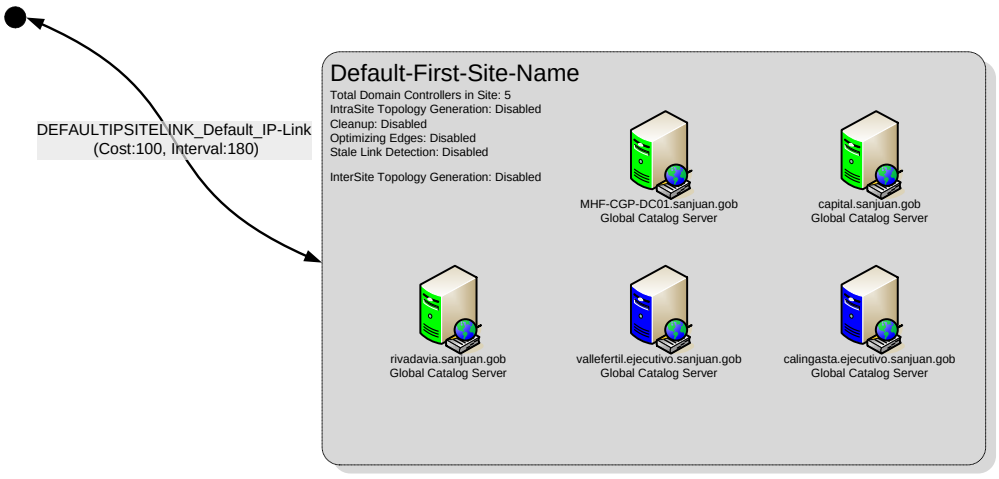


Figura 5 – Vinculación y replicación entre Sitios

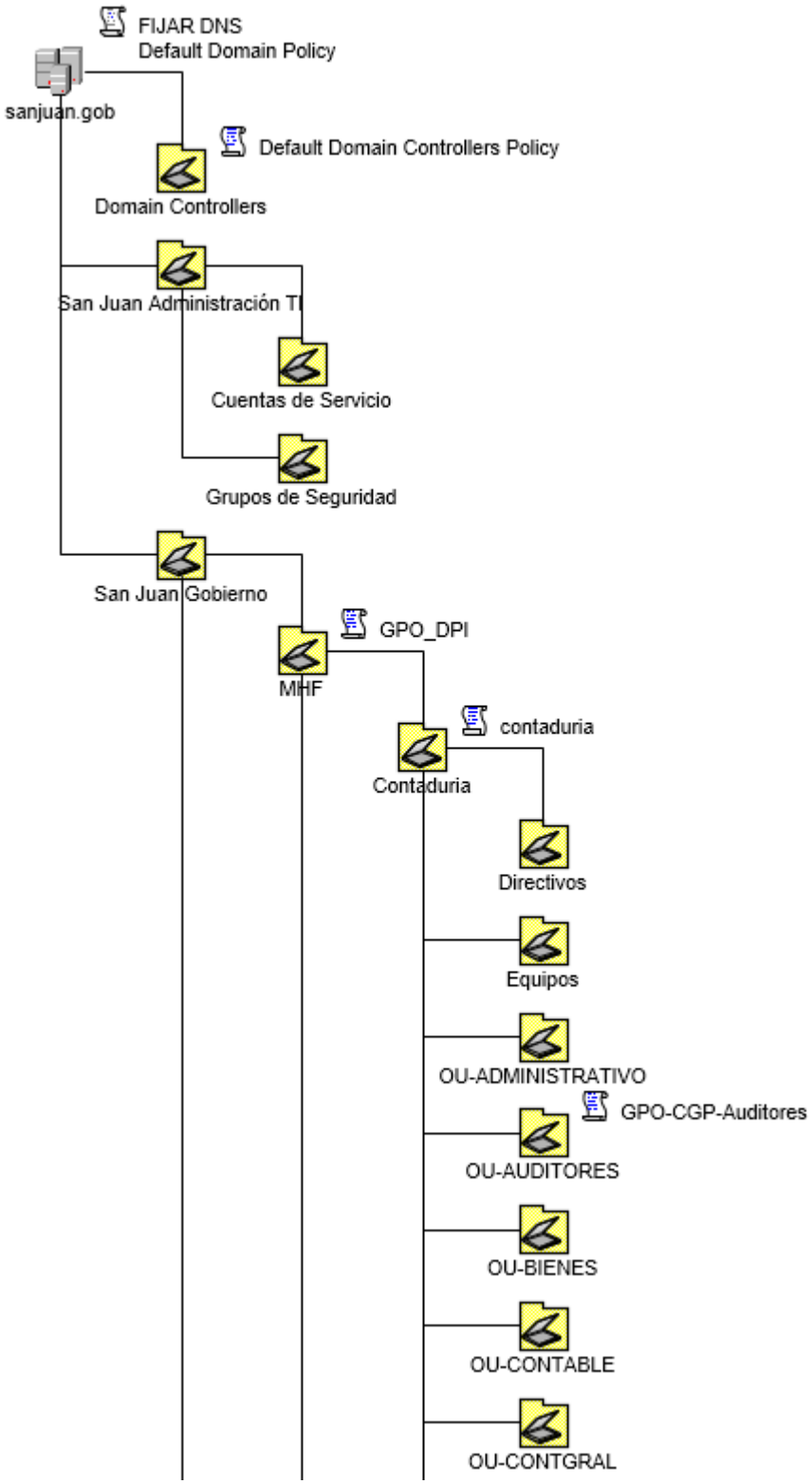
Actualmente, los servicios de directorio estudiados tienen definidos un solo sitio cada uno. En el caso del relevamiento realizado es claro ver la existencia del sitio por defecto. Debido a los requerimientos actuales, se considera que no es necesario modificar esta fase de diseño. Ahora bien, el diseño de sitios consiste en el mapeo de las redes físicas en la construcción de sitios lógicos del servicio de directorio. Un sitio en Active Directory es una colección lógica de una o más subredes TCP/IP bien conectadas. También se puede entender a los sitios del directorio como la representación lógica de la distribución física de los componentes del directorio.

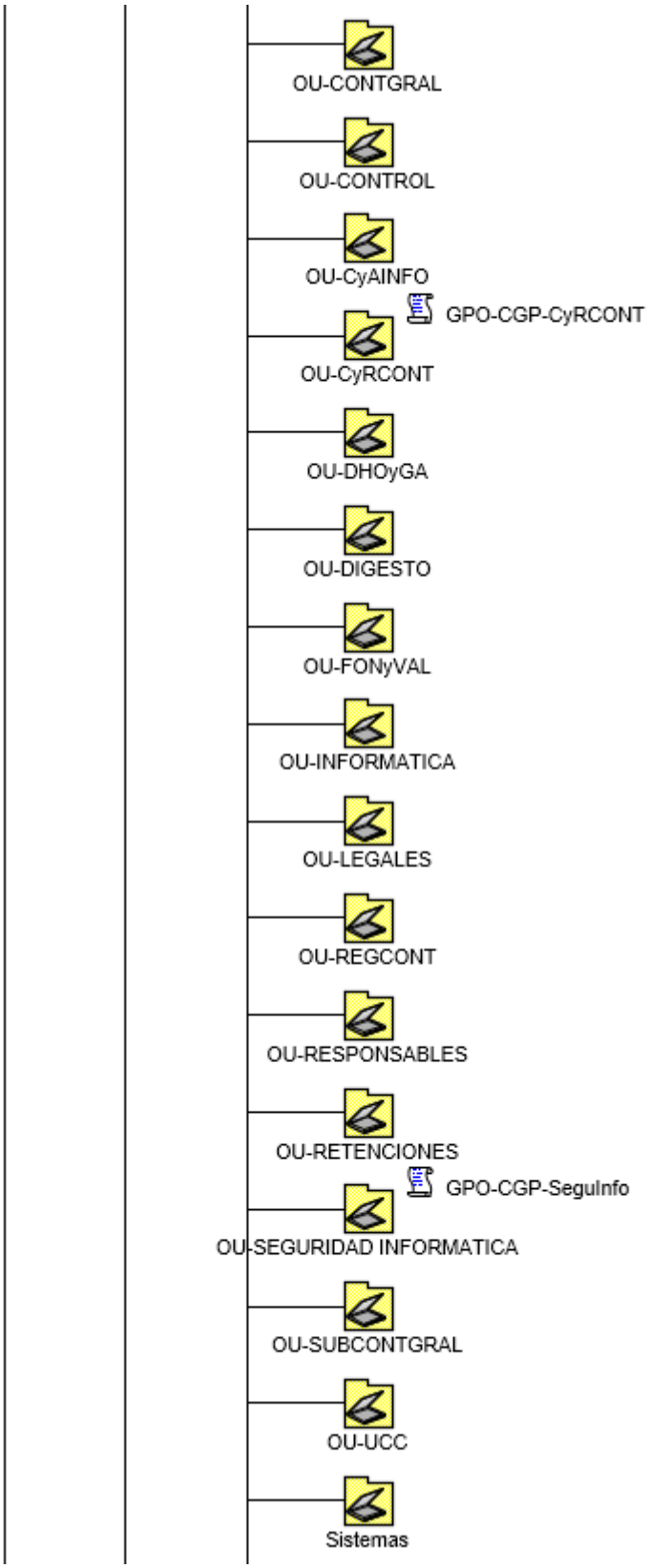
Los Sitios se utilizan para controlar la replicación del directorio mediante el establecimiento de un calendario para la replicación entre sitios. También se utilizan para dirigir los clientes del directorio hacia los recursos de red más cercanos relacionados con el directorio.

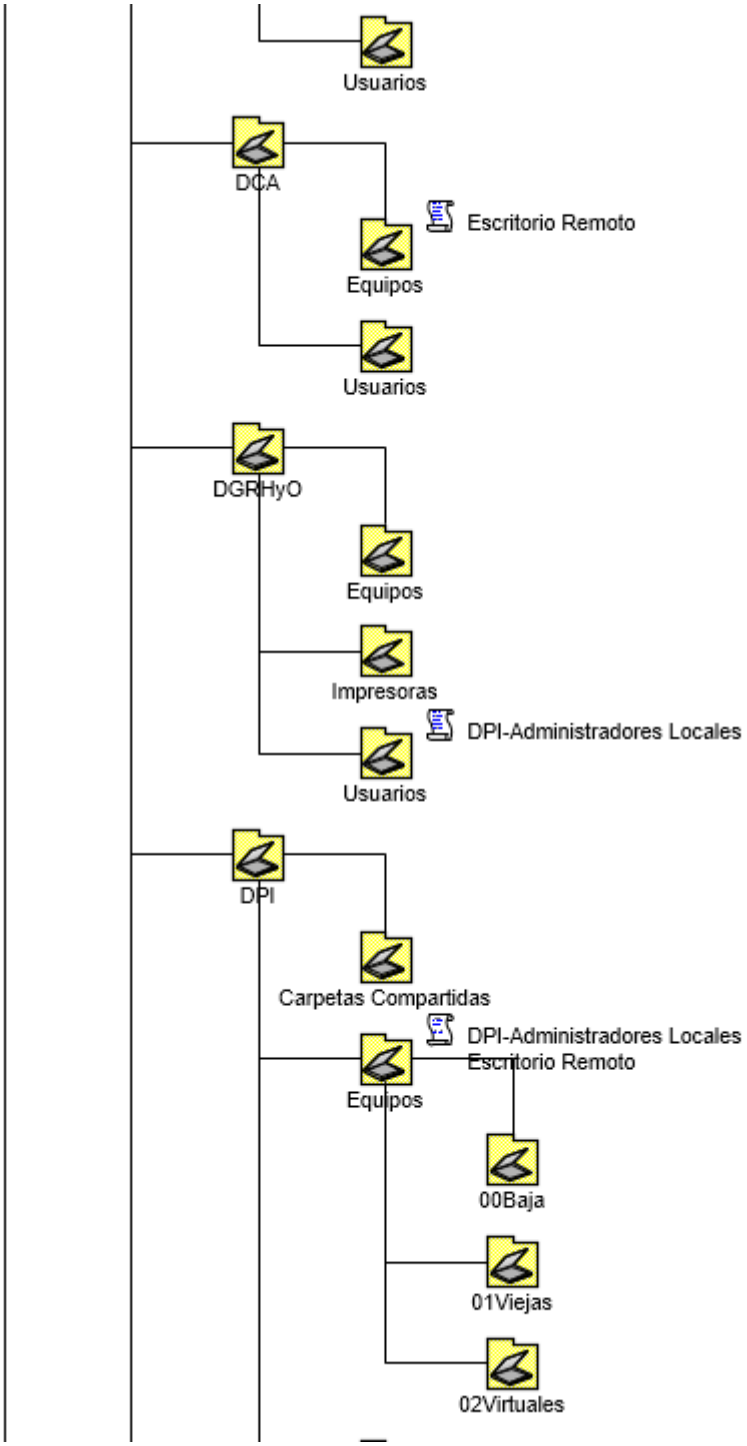
Es importante comenzar a identificar la totalidad de los sitios definidos en la totalidad de los servicios de directorio de gobierno, e iniciar el mapeo de las subredes TCP/IP representadas en una ubicación específica de los sitios correspondientes.

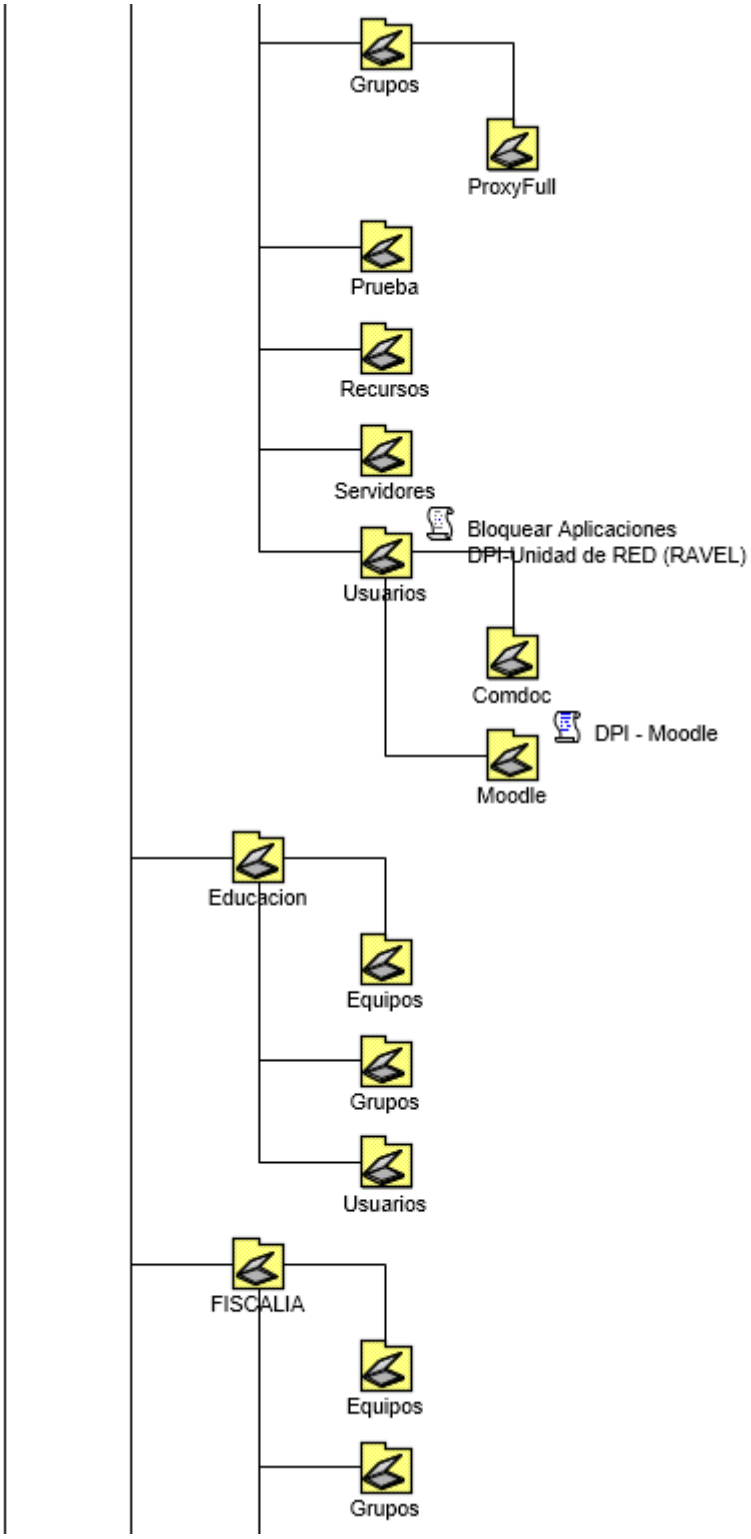
Objetos y Políticas de Grupos del Dominio “sanjuan.gob”

A continuación, se presenta el relevamiento de objetos y políticas existentes del dominio raíz “*sanjuan.gob*”.




OU-CONTGRAL
OU-CONTROL
OU-CyAINFO
GPO-CGP-CyRCONT
OU-CyRCONT
OU-DHOyGA
OU-DIGESTO
OU-FONyVAL
OU-INFORMATICA
OU-LEGALES
OU-REGCONT
OU-RESPONSABLES
OU-RETENCIONES
GPO-CGP-SeguInfo
OU-SEGURIDAD INFORMATICA
OU-SUBCONTGRAL
OU-UCC
Sistemas


Usuarios
DCA
Escritorio Remoto
Equipos
Usuarios
DGRHyO
Equipos
Impresoras
DPI-Administradores Locales
Usuarios
DPI
Carpetas Compartidas
DPI-Administradores Locales
Escritorio Remoto
Equipos
00Baja
01Viejas
02Virtuales


Grupos
ProxyFull
Prueba
Recursos
Servidores
Bloquear Aplicaciones
DPI-Unidad de RED (RAVEL)
Usuarios
Comdoc
DPI - Moodle
Moodle
Educacion
Equipos
Grupos
Usuarios
FISCALIA
Equipos
Grupos

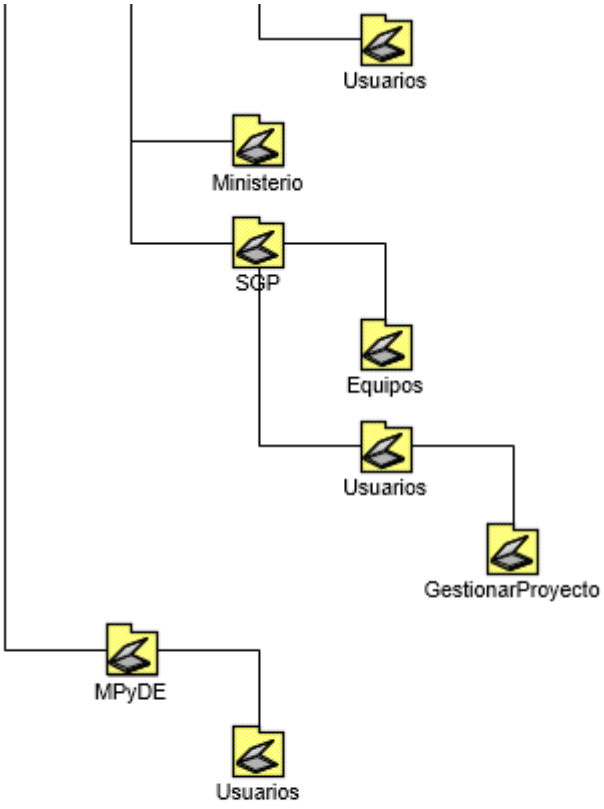


Figura 6 – Objetos y Políticas de Grupos – Dominio “sanjuan.gob”

Objetos y Políticas de Grupos del Dominio “ejecutivo.sanjuan.gob”

A continuación, se presenta el relevamiento de objetos y políticas relevadas del dominio “*ejecutivo.sanjuan.gob*”.

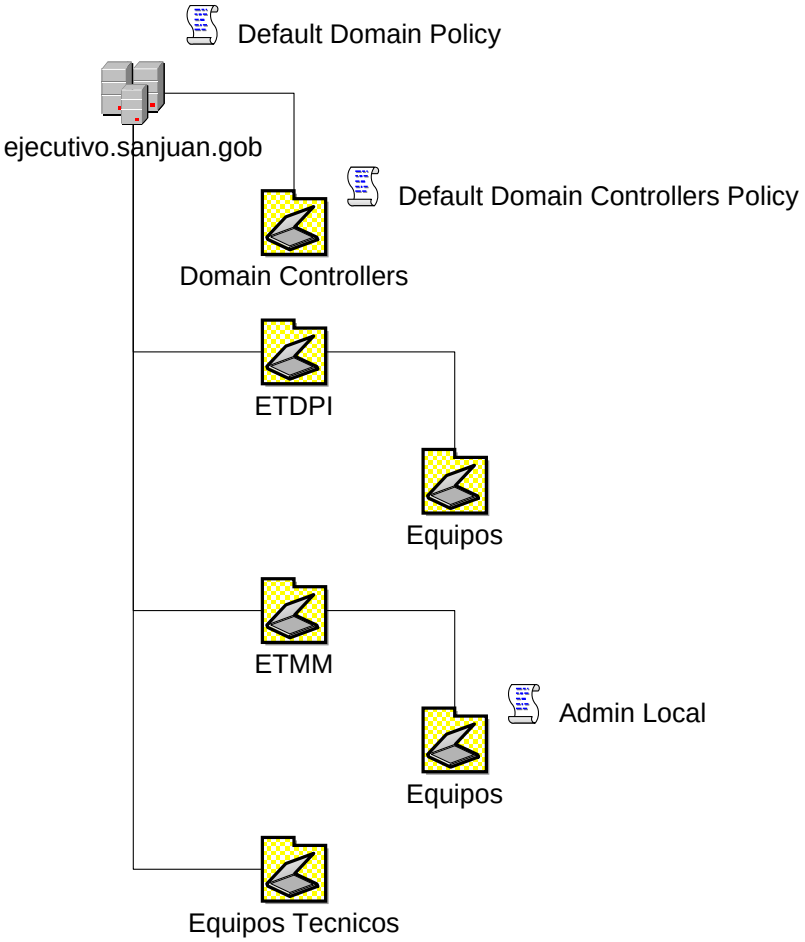


Figura 7 – Objetos y Políticas de Grupos – Dominio “ejecutivo.sanjuan.gob”

Layout de la infraestructura TI asociada al Servicio de Directorio

La Secretaría de la Gestión Pública (SGP), ha llevado a adelante una política de implementación y despliegue de Tecnología Informática (TI) a nivel del Poder Ejecutivo Provincial. Lo descripto se efectúo en base a un análisis global desarrollado y evolucionado durante varios años. Esta política planteaba, entre sus numerosos objetivos, el de brindar Servicios TI de carácter global y transversal en el ámbito del poder mencionado. Es decir que servicios esenciales a nivel de TI para la

integración e interacción de las diversas áreas o reparticiones dentro de Gobierno, sean provistos coordinadamente.

A continuación, se presenta el diagrama con la infraestructura implementada en la actualidad asociada al servicio de directorio en estudio.

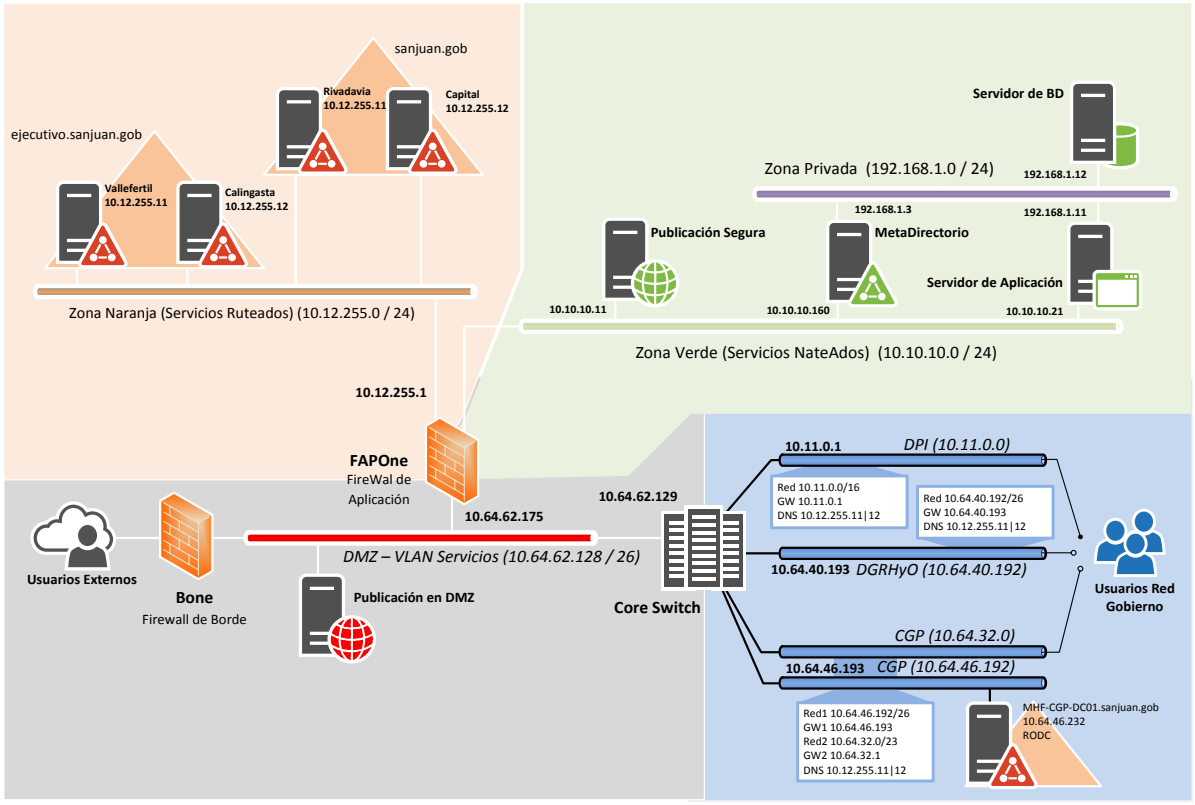


Figura 8 – LayOut Infraestructura TI actual.

Este diagrama solo representa una parte de la configuración lógica de la red global de Gobierno. Es oportuno aclarar que el alcance del mismo está acotado a la infraestructura de servicios TI relacionados al Servicio de Directorio.

En esta figura se visualiza la integración/vinculación con la red interna del edificio la cual es definida por el Core Switch administrado por la Dir. de Conectividad y Telecomunicaciones dependiente del Ministerio de Infraestructura y Servicios Públicos. Es bueno aclarar que el resto de la Infraestructura presentada es administrada por la Secretaría de la Gestión Pública.

Este esquema presenta parte de la conectividad física a nivel de Capa3, como así también su segmentación desde un punto de vista de perímetros y redes de seguridad.

Las subredes en color azul involucran la mayoría de los accesos de usuarios internos de gobierno que se encuentran conectados al hub central en el centro de Datos (Core Switrch). Se conoce como todo lo que se encuentra “detrás” del Core Switch.

También es posible visualizar uno de los accesos a Internet (Usuarios externos) con los cuales actualmente cuenta Gobierno. Este acceso se realiza a través del Firewall de Borde (BOne – Border One), el cual es un servicio simétrico y corresponde al acceso principal. Sobre este se brinda el servicio de navegación a internet (Protocolo http puerto 80 principalmente) y la posibilidad del servicio de publicación WEB de ser necesario.

También se visualiza la denominada Zona Naranja. Esta subred representa el ámbito fundamental donde se ha desplegado el Servicio de Directorio. Se a implementado en Gobierno el servicio de directorio Active Directory de Microsoft. Este servicio es uno de los pilares básicos sobre los cuales se implementa toda infraestructura tecnológica. De esta forma, Gobierno ha llevado adelante la consolidación de este servicio. La mencionada consolidación se implementó sobre un Sistema IBM Pureflex, también conocido como Flex System. Este sistema de cómputo cumple ampliamente con los requerimientos necesarios para dar soporte a un Servicio de Directorio como el aquí descripto. Esta zona Naranja tiene la particularidad de poder direccionarse mediante ruteo de capa 3. Es decir, que el acceso se logra mediante ruteos simples empleando el protocolo TCP/IP. Lo anterior es lo recomendable para directorio y servicios de infraestructura similares.

También es posible visualizar dos redes complementarias, las cuales son la red Verde y la red Morada. La red Verde denota la red segura. La red sobre la cual se implementarán los sistemas de información a proveer u alojar, como así también servicios tanto de infraestructura como de básicos de TI. La particularidad de esta red es la seguridad, por lo cual está configurada para accederla mediante la implementación del protocolo NAT (*Network Address Traslation*). La red Morada se encuentra detrás de la red verde y solo es accesible por los equipos definidos como

ForntEnd en las arquitecturas de sistemas y servicios. Estas dos redes permiten la implementación de una infraestructura segura, acorde a ámbitos de nivel gubernamental. La red morada, es una red privada, solamente accesible mediante los servidores de aplicación.

La infraestructura descripta se complementa con un dispositivo especial que es el Firewall denominado FApOne (FireWall Aplicactions One). Este es un Firewall de Aplicaciones, y ha sido implementado empleando un producto de software libre. La versión empleada es PFSense, el cual es factible de clasificarlo como un UTM por software, que funciona perfectamente en ambientes virtualizados.

La tecnología implementada, responde a un esquema de arquitectura de Infraestructura TI capaz de soportar y brindar servicio a un ámbito gubernamental como el de la Provincia de San Juan. El diseño en capas y la segmentación implementada, permite la posibilidad de ir potenciando cada uno de los componentes involucrados, para alcanzar la escalabilidad de la infraestructura. Es factible, mediante el cumplimiento de ciertas premisas, poder ir intercambiando determinados componentes, a fin de ir potenciando la arquitectura implementada.

Diseño del Servicio

De los diversos servicios de directorio existentes en la actualidad en el Poder Ejecutivo Provincial, existe una implementación que ha sido diseñada bajo la visión de escalabilidad y transversalidad para brindar un servicio integral. Esta instancia desplegada desde la Secretaría de la Gestión Pública debería ser tomada como base para llevar a cabo el desarrollo y evolución de un servicio de escala, acorde al Gobierno Provincial.

El diseño adoptado para esta instancia fue concebido bajo premisas tendientes a ofrecer un servicio de nivel corporativo. Es importante aclarar que la realidad política y económica del ámbito donde se desarrollará el proyecto de implementación del servicio ha cambiado. Y este cambio debe ser considerado, y evaluado oportunamente a fin de adaptar el diseño para ajustarse a la nueva realidad.

El alcance inicial concebido del diseño lógico fue la cobertura de la SGP. Previendo contar con capacidad de crecer (escalar) para brindar servicio al resto del ejecutivo provincial.

El servicio tiene la capacidad de ser entregado transversalmente a toda la organización. Es decir que pueda ser consumido desde cualquier sitio y por cualquier unidad organizacional que forme parte del Ejecutivo Provincial. Inclusive existe la posibilidad de extender su alcance a estructuras semejantes como pueden ser los otros poderes (Judicial y Legislativo), u otras organizaciones como pueden ser Municipalidades o entidades similares. El concepto de un servicio único y transversal está contemplado en este diseño.

En el ámbito del ejecutivo provincial se encuentra una amplia base de instancias operativas Windows instaladas. Se puede considerar como el Sistema Operativo único desplegado. Existen implementaciones de sistemas operativos alternativos, como son algunas distribuciones de Linux, pero en un número no considerable. De todos modos, es factible la integración de estas distribuciones mediante el despliegue del protocolo LDAP. No siendo el alcance de esta consultoría llevar a cabo un análisis comparativo de los servicios de directorio, Active Directory es una de las soluciones más desarrolladas y maduras que actualmente se encuentran en el mercado. En forma complementaria, este directorio pose un entorno operativo ampliamente integrado con diversos sistemas y servicios TI existentes en el ámbito público. Siguiendo este enfoque, esta consultoría aconseja continuar con la implementación existente de Active Directory, migrándolo hacia un nuevo diseño debidamente adecuado al nuevo escenario.

Active Directory posee extensa documentación y procesos respaldados en una Arquitectura de Referencia. De esta forma una vez que se defina el modelo organizacional, y respetando las premisas y requisitos de diseño es factible comenzar a avanzar en el seguimiento de las guías que aporta la mencionada arquitectura. Este proceso asegura la definición de una solución adecuada a los estándares, y con una madurez ya probada en diferentes ambientes similares al gubernamental.

Definición del Modelo Organizacional – Servicio de Directorio

El Modelo Organizacional inicial propuesto a adoptar fue el del CDC (Centro de Datos Centralizado. Se empleó la infraestructura existente en el Centro de Datos

existente en el 1º subsuelo del edificio del Centro Cívico. Desde allí se proveen los servicios TI en forma centralizada, mediante el empleo de la red física existente (Capa 1). Todas las dependencias como son ministerios, secretarías, direcciones y demás reparticiones; deberían consumir servicios desde el Centro de Datos mencionado (bajo el modelo de CDC). En forma complementaria y ante un crecimiento futuro, distintas unidades de gobierno existentes en sitios remotos podrían crecer bajo el concepto de Unidades. Algunas de estas unidades podrían definirse como Unidades Satélites.

Por la naturaleza misma de una organización como es Gobierno, por su tamaño y complejidad, el diseño es capaz de ser flexible. Es decir, soportar en un futuro el crecimiento hacia dos modelos adicionales. Estos dos modelos serían el de Departamento y el de IDC. El de Departamento deberá incorporarse en la medida que se evolucione en requerimientos de seguridad y aislamiento. Estos requerimientos irán surgiendo naturalmente. El Servicio de Directorio Active Directory, posee estructuras lógicas perfectamente definidas que permiten la implementación de este modelo.

Complementariamente, si bien el Modelo CDC contempla la capacidad de poseer una presencia básica de servicios en internet, la tendencia es hacia el concepto de Gobierno Abierto. Este concepto está enunciado como un nuevo modelo de distribución de servicios, orientado a lo que abarca el Modelo IDC.

La metodología propuesta de modelado a partir del concepto de prestación y consumo de servicios contempla adecuadamente la posibilidad de ir creciendo y abarcando los distintos modelos planteados. Como ya se ha comentado, una organización con el volumen y complejidad como lo es Gobierno requerirá la adopción de todos los modelos de organización presentados. Y sin dudas las herramientas empleadas permiten llevar a cabo el despliegue y adecuación de las implementaciones futuras.

Diseño Lógico Propuesto

A continuación, se presenta un diagrama que detalla los componentes lógicos necesarios para desplegar un servicio acorde a las especificaciones y requerimientos enunciados.

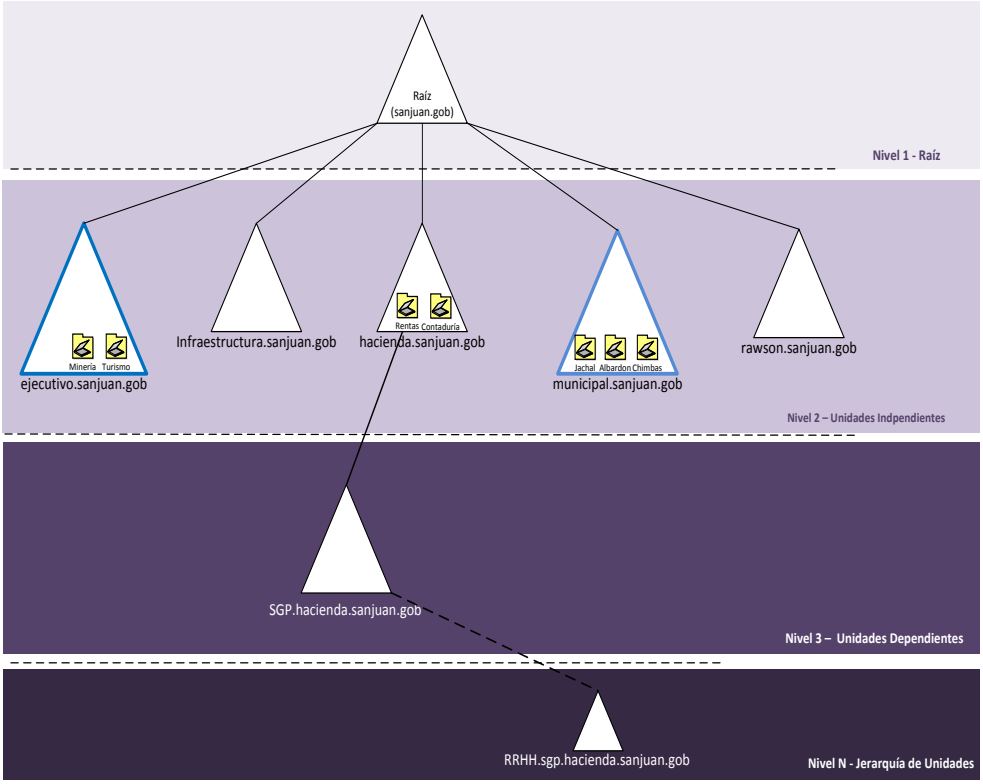


Figura 9 - Diseño lógico adoptado

Este diseño define una capacidad lógica de crecimiento y/o escalabilidad. Esta escalabilidad debe ser entendida tanto en el sentido vertical como horizontal.

Se ha definido inicialmente un solo bosque. Este bosque tendrá como raíz un dominio el cual contendrá objetos que tengan incumbencia transversal a la organización, es decir al Poder Ejecutivo Provincial. O quizás puede ser ampliado al Gobierno de San Juan, o la Administración Pública Provincial. Esta raíz tiene asociado el nombre de dominio “sanjuan.gob”. De esta forma queda definido el primer Nivel (Nivel 1).

Luego en un segundo Nivel (Nivel 2) se ubican las Unidades Independientes. Se entiende por Unidades Independientes aquellas que poseen la madurez técnica y funcional para administrar un dominio propio. Aquí se refiere estrictamente al concepto de domino dentro del ámbito de Active Directory. De esta forma se asegura la escalabilidad horizontal, es decir que es factible incorporar la cantidad necesaria de divisiones, en este caso Dominios, para responder a las necesidades o requerimientos futuros. Es bueno aclarar que el incremento de dominios conlleva un aumento en la complejidad, y en especial un costo adicional asociado a la asignación de hardware específico para soportar esa nueva unidad lógica.

El modelo de administración propuesto propone, contenedores especiales (Dominios de Active Directory) que permitirán un crecimiento inicial. Estos dominios particulares, denominados inicialmente **Dominios de Organización**, están representados por triángulos azules en el diagrama. Estos dominios permitirán englobar la administración de organizaciones en un estadio inicial, o de aquellas que no posean la madurez técnica necesaria para administrar su propio dominio. Estos Dominios de Organización irán creciendo o incorporando organizaciones, mediante la creación de Unidades Organizativas para asegurar la independencia necesaria. Veamos el diagrama del diseño lógico presentado en la Figura 9. En este, el Dominio de Organización "*ejecutivo.sanjuan.gob*" contendría a todas las reparticiones que inicialmente pertenecen al Poder Ejecutivo de la Provincia. En el diagrama se han modelado dos ministerios a modo de ejemplo. Estos son el ministerio de Minería y el de Turismo. Para estos dos Ministerios se crearían dos Unidades Organizativas (UO), una para cada uno. Estas UOs permitirían aislar los objetos propios de cada ministerio, simplificar notablemente la administración y minimizar sensiblemente la inversión en hardware necesaria para respaldar el modelo lógico.

Un aspecto importante para tener en cuenta es determinar la granularidad necesaria para el modelado. Qué nivel de representación mínima se le asignará a una UO. Desde esta consultoría se consideró, que un criterio adecuado puede ser el definir un Ministerio como el nivel máximo representación de una UO, y el mínimo sea una Dirección. Este criterio definido, debe ser considerado también en organizaciones similares al poder ejecutivo provincial y su equivalencia a nivel organizativo. De esta forma el posible escalar la estructura del servicio a otros tipos de organizaciones. Desde un punto de vista de políticas de gestión, tiene bastante

lógica lo planteado en el punto anterior. Este tipo de políticas administración y operación de servicios TI son comunes a nivel de Dirección en el ámbito de la Administración Pública Provincial (APP en adelante). La administración de usuarios, credenciales y políticas asociadas se definen naturalmente en ámbitos acotados a una Dirección. Puede existir un caso particular en el que sea necesario definir una granularidad menor, como puede ser el nivel de sección o de división. Pero esto último no es aconsejable desde el punto de vista del esfuerzo asociado a la administración de esa granularidad. Ese nivel de granularidad debe ser enfocado o atendido empleando políticas específicas, políticas a nivel del servicio, y no trabajándolo con unidades organizativas.

En un futuro, si los requerimientos de uno de estos ministerios creciesen en algún aspecto, sería posible escalar hacia un domino exclusivo. Este sería el caso del dominio “hacienda.sanjuan.gob” que figura en la Figura 9 (Ministerio de Hacienda y Finanzas). De ser necesaria una especialización mayor se puede crecer a un nuevo nivel hacia abajo, como sería el caso del dominio “SGP.hacienda.sanjuan.gob” (Secretaría de la Gestión Pública dependiente del Ministerio de Hacienda). Este crecimiento vertical permite establecer un nivel de especialización y modelado más detallado de la organización.

Este modelo de diseño propuesto conlleva un diseño amplio con el fin de abarcar al resto de las organizaciones gubernamentales a nivel provincial, de ser necesario. Es bueno aclarar que, en el esquema del ejemplo presentado, se ha desarrollado un crecimiento vertical siguiendo la jerarquía natural del organigrama de Gobierno. Esto es con el fin de facilitar su interpretación. Ahora bien, lo deseado es lograr adaptar el escalamiento tanto horizontal como vertical desde una visión de requerimiento y provisión de servicios TI. Desde la madurez en aspectos de provisión de servicios de TI que posee la organización. Es decir, considerando la naturaleza de un servicio de directorio de red. La ceración de un nuevo Dominio o Unidad Organizativa debería depender exclusivamente del nivel de desarrollo de esa unidad u organización para la provisión o requerimientos asociados al servicio de directorio.

Estructura Organizacional del SD.

Debido a la importancia y trascendencia de este tipo de Servicio, y el alcance que se le ha dado, se ha intentado consolidar la fuerza de trabajo asociada. Se inició el trabajo de especificación de los roles asociados a la operación y administración del Servicio a nivel de la Dirección Provincial de Informática dependiente de la SGP, en forma conjunta con el staff técnico del Ministerio de Educación. Este grupo, trabajó colaborativamente en la consolidación de la gestión del Servicio.

A continuación, se presenta el enfoque de la OBS (en inglés Organization Break Down Structure) definida oportunamente. Esta sigla refiere a la descomposición de la estructura organizacional. Se pueden representar las personas asignadas o las funciones que representan esas personas. Se consolidó el trabajo a nivel de funciones o lo que denominaremos “roles”.

Basándose en la documentación del producto y tomando indicadores relacionados con el ámbito de la administración pública, donde se implementó el servicio, se respetó la siguiente enumeración de roles asociados a la administración, soporte y operación del servicio de directorio.

Roles	Descripción
Administrador de Infraestructura	Administración de la infraestructura TI física y lógica asociada al servicio de directorio. Abarca la totalidad de componentes servidores (virtuales y físicos). Sistemas Operativos de Red (NOS), Hypervisores, y demás tecnologías complementarias asociadas.
Administrador de Conectividad y Comunicaciones	Administración de la conectividad y comunicaciones como soporte a la infraestructura asociada al servicio. Incluye la capa de seguridad de redes de redes y activos.

Administrador del Servicio	Administración del Servicio de Directorio propiamente dicho. El alcance de este rol abarca el bosque, dominio raíz y los dominios de organización. No incluye las OU independientes, debido a que estas están a cargo de sus respectivos administradores.
Gestor de Documentación y Enlace.	Definición de mejores prácticas y procedimientos que empleará el equipo central. Esta área debe refinar y definir la base de procedimientos y prácticas a emplearse. Debe mantener la documentación asociada y será responsable de la educación y formación de usuarios. (Subdominios, Unidades Independientes, Unidades Organizativas, etc.).
Auditor Interno	Análisis de servicios de infraestructura TI. Colaborar como consultor con el ámbito auditado. Generación de ideas de cómo enfocar la construcción de los elementos de control y de gestión, actuando como consejero con la organización. Generación de informes periódicos y realización de mediciones. Este es el único rol que, si bien está especificado, no se ha llevado a su implementación.

Tabla 1 – Descripción de Roles.

A continuación, se enumerarán ciertos criterios que son necesarios para entender la propuesta de roles existentes:

Actualmente en el ámbito del Poder Ejecutivo Provincial no existe una única área con la capacidad y el alcance de poder llevar a cabo el despliegue del Servicio de Directorio en forma integral. Lo anterior determina que el despliegue se realiza mediante la colaboración de las áreas involucradas.

Es conveniente conformar una fuerza de trabajo con capacidad técnico/operativo, para administrar un servicio transversal al ejecutivo provincial definido en el alcance del proyecto. Por la naturaleza del servicio será necesaria indefectiblemente la interacción entre las distintas áreas de TI involucradas.

Un aspecto importante que considerar son las buenas prácticas propuestas por el fabricante del servicio. Lo anterior refiere a la necesidad de analizar la división del rol del Administrador del Servicio. Este Administrador engloba dos actividades importantes, como es la administración del Servicio y la administración de los Datos. Esto deberá ser analizado detalladamente en conjunto con las autoridades técnicas de Gobierno, a fin de consolidar la estructura organizacional necesaria para consolidar la provisión del Servicio.

Limitaciones y realidades actuales

El crecimiento de este servicio a futuro es prometedor, en la medida que se vayan cumpliendo los objetivos planeados. Así, un factor determinante será la capacidad de dar soporte a una gran cantidad de usuarios de diversas áreas de distintos ministerios.

Es fundamental iniciar el desarrollo de determinadas capacidades entre los integrantes de la administración del servicio. Esta capacidad tiene que ver con I+D, Documentación técnica y de procesos, auditoría y control, entre otras.

De esta forma se inicia el aseguramiento de la interacción de los componentes *Personas/Tecnología/Procesos,* según el enfoque teórico presentado.

Debido a la sensibilidad desde un punto de vista de seguridad organizacional que involucra naturalmente el servicio de directorio, es que se torna fundamental la creación de un área de auditoría a nivel de servicio. Inicialmente sería aconsejable que esa área acompañe a las áreas técnicas en el desarrollo de procesos y herramientas necesarias para llevar a cabo la auditoría correspondiente.

Por la envergadura de este Servicio, será fundamental el desarrollo del área de soporte o Mesa de Ayuda. Esta área debería operar integrada con otros servicios fundamentales como son por ejemplo el servicio de conectividad y comunicaciones. La propuesta es la de implementar un servicio de soporte en 3 niveles. Con la dinámica de ir escalando al siguiente nivel en función de la complejidad del incidente reportado.

Nivel de Soporte	Detalle
Soporte Nivel 1	Mesa de Ayuda. Soporte al usuario general. Soluciones de acceso al servicio y uso del mismo. Educación del usuario
Soporte Nivel 2	Administración de objetos. Soporte e interacción con Administradores de objetos y Contenedores delegados. Soporte a pares.
Soporte Nivel 3	Área de I+D. Interacción con Expertos. Responsables de la Disponibilidad. Administración del Bosque y Dominios de Organización.

Tabla 2 – Niveles de Soporte.

Nota: El servicio de directorio es un servicio en constante evolución y de una complejidad elevada. Es considerado, sin duda, como un servicio de misión crítica dentro de las organizaciones modernas. Debido a lo anterior, se torna fundamental la contratación de un servicio de soporte provisto por el fabricante de la solución o un asociado debidamente certificado. El tercer nivel de soporte debería ser el encargado de interactuar (o escalar) con este proveedor o el fabricante.

Partiendo de la base de poder contar con Sistemas Integrados, y complementariamente disponer de la posibilidad de vincularlos a un Servicio de Directorio (como repositorio central de Infraestructura TI); es conveniente comenzar a analizar los procesos asociados a la gestión de usuarios. Lo anterior a fin de determinar el método a seguir para lograr la integración o vinculación de la gestión de usuarios.

Sistema de Gestión Documental

El Sistema de Gestión Documental adoptado por la SGP es el SIGED. El mismo es un sistema esencialmente desarrollado para el seguimiento de procesos asociados a Expedientes. Facilita enormemente poder efectuar la trazabilidad del documento o expediente, registrando cada uno de los pasos que el mismo va siguiendo. Al momento del inicio de esta consultoría, se iniciaba la implementación y despliegue del SIGED. En el ámbito del ejecutivo provincial, existían numerosos sistemas que cumplían funciones similares. Fue una decisión acertada de la SGP iniciar el proceso de integración y migración de los sistemas existentes hacia uno único y centralizado. Este sistema sería el SIGED como ya se mencionó.

El equipo que integra esta consultoría estuvo a cargo de un proceso similar hace un par de años, también en el ámbito de la SGP. Así, una de las funciones importantes asignadas, fue el participar y colaborar a modo de consultores en todo lo que fuese necesario para contribuir con el despliegue del SIGED. Y fundamentalmente asistir al equipo de trabajo encargado del despliegue e implantación.

Complementariamente a lo descripto en los párrafos anteriores, en base a la experiencia en ámbitos gubernamentales, se propuso iniciar un enfoque global hacia procesos. Comenzar a trabajar en la gestión asociada a procesos. Es así como se planteó la identificación de procesos centrales y transversales. A continuación, se presenta este enfoque orientado a un conjunto de procesos centrales por excelencia en el ámbito de la Gestión Pública, que integra los ejes de la presente consultoría. Este es el conjunto de procesos orientados a la identificación de personas/usuarios/agentes de manera unívoca a nivel de la Administración Pública Provincial (APP).

Procesos

Interacción de procesos relacionados con personas/usuarios

Un objetivo central de la SGP, en su política actual, es poder desarrollar las bases para la identificación de personas/usuarios/agentes de manera unívoca a nivel de la APP. Este proceso unificado de identidad conlleva el desarrollo de una integración ordenada y planificada de Sistemas de Información y Servicios de TI.

En lo relacionado con los Sistemas de Información se han tomado decisiones importantes, y una de las centrales es la integración de los mismos. Es decir, se trabaja en el desarrollo e implementación de Sistemas Integrados. En lo referido a las personas, en el más amplio de los sentidos bajo un alcance provincial, se trabaja en el desarrollo de dos sistemas principales. Estos son el Sistema de Identificación de Personas (SIP) y el Sistema Integrado de Administración de Recursos Humanos (SIARH). El resto de los sistemas a desarrollar y modernizar se vincularán de diversas formas con estos dos sistemas.

Al referirnos a los Servicios TI, surge naturalmente la necesidad también de centralizar la gestión de usuarios en un servicio. Es natural, y aconsejable respaldándose en las mejores prácticas, que ese servicio sea el Servicio de Directorio.

Así ambos entornos, tanto Sistemas como Infraestructura, idealmente deberían poseer una correlación unívoca en lo referido a la identificación y seguimiento de usuarios y sus perfiles asociados.

El camino propuesto es trabajar en el establecimiento de relaciones fuertes y bien definidas, entre los dos sistemas (SIP y SIARH) y el Servicio de Directorio central de infraestructura propuesto.

Formularios Asociados

Así, en base a lo planteado, se realizó una recopilación de formularios actualmente vigentes. Estos formularios son los asociados a la gestión de los Sistemas Integrados y la administración de usuarios de servicios TI en el ámbito de la SGP. Dichos documentos fueron desarrollados oportunamente, en su mayoría, por el Área de Seguridad Informática dependiente de la Contaduría General de la

Provincia de San Juan. Complementariamente, se incluye el formulario de “Solicitud de una Cuenta de Correo Electrónico”. Este último fue desarrollado por el Área de Servicios TI de la Dirección Provincial de Informática (DPI) dependiente de la SGP. Es el empleado para gestionar actualmente el proceso de alta de usuarios en el servicio de Correo Electrónico. Si analizamos este proceso, observaremos que involucra la creación de un usuario en el Servicio de Directorio que tiene asociado el dominio de internet “sanjuan.gov.ar”.

Así, es central a la hora de analizar la integración de Sistemas y Servicios, lo cual es uno de los objetivos de la presente consultoría como ya se manifestó.

Luego del relevamiento realizado, se presenta la siguiente tabla con el detalle de los formularios existentes bajo el alcance mencionado.

El encabezado está constituido por la siguiente información: N° de Fila **[N°]** – Código del Formulario **[Cod]** – Nombre o Descripción del Formulario **[Nombre/Descripción]** – Formato del Formulario (extensión del formato de archivo) **[Form]** – Versión del Formulario **[Versión]** – Fecha de la Versión del Formulario **[Fecha V]** – Cantidad de páginas que posee el Formulario **[Pág]**.

La tabla con los Formularios relevados es la siguiente:

N°	Cod	Nombre / Descripción	Form	Versión	Fecha V	Pág.
1	F100	Compromiso De Confidencialidad	.docx	N/D	N/D	1
2	F101	Solicitud De Usuario/Clave Para Acceso A Sistema Integrado S.I.I.F.	.docx	6.2	N/D	1
3	F101B	Descripción Tareas Habilitado Para SIIF	.docx	1.0	Oct 2013	1
4	F103	Solicitud De Cambio Y/O Desbloqueo De Contraseñas	.docx	6.0	Abr 2014	1
5	F104	Solicitud De Contraseña Para Implementador	.docx	N/D	N/D	1
6	F105	Solicitud De Perfil De Usuario De Emergencia (P.U.E.)	.docx	N/D	N/D	2
7	F106	Comunicación De Usuario Y Clave	.docx	N/D	N/D	1
8	F107	Prueba Controlada De Contingencia	.docx	1.0	Oct 2013	2
9	F109	Solicitud De Requerimiento De Informe	.docx	4.0	Abr 2015	1
10	F111	Solicitud De Usuario/Clave Para Acceso A Sistema Integrado	.docx	6.2	Ago 2016	1
11	F112	Solicitud De Usuario/Clave Para Acceso A Sistema Integrado S.I.G.O.P.	.docx	6.2	Ago 2016	1
12	F113	Solicitud De Usuario/Clave Para Acceso A Sistema Integrado I.P.V.	.docx	6.2	Ago 2016	1
13	F114	Solicitud De Usuario/Clave Para Acceso A Sistema Integrado S.I.Ge.D.	.docx	6.2	Ago 2016	1
14	F115	Solicitud De Usuario/Clave Para Acceso A Sistema Integrado S.I.A.R.H.	.docx	6.2	Ago 2016	1
15	S/N	Solicitud De Una Cuenta De Correo Electrónico	.pdf	4.0	N/D	2
16	F101D	Versión Digital del Formulario F101	.pdf	N/D	Oct 2016	1

Tabla 3 – Listado de Formularios Relevados.

Nota: *al final del informe se presenta la sección Anexos. Esta sección incluye una tabla donde se detallan los archivos adjuntos al presente informe incluidos en el CD que acompaña.*

A partir del avance del proyecto de desarrollo del Sistema Integrado a nivel de la Administración Pública Provincial (APP), y en particular en el ámbito de la Secretaría de la Gestión Pública (SGP), se ha comenzado a trabajar en la actualización y rediseño de los formularios aquí descriptos. Este trabajo se realiza en conjunto entre las áreas de Seguridad, de Desarrollo de Software y los proyectos en ejecución SIIF

y SIGED particularmente. Complementariamente sería aconsejable interactuar con los equipos que trabajan en el diseño de los sistemas SIP y SIARH.

Procesos involucrados

Estos formularios, definen procesos definidos particularmente desde un punto de vista funcional. Si se analiza detalladamente, para citar un ejemplo, varios de ellos involucran altas de usuarios de concepciones muy similares, y configuraciones también asociadas a usuarios. De aquí se desprende la relación entre el conjunto de formularios F101, F111 al 115 y la Solicitud de una cuenta de Correo Electrónico. Todos estos formularios involucran un subproceso particular que es la creación de un usuario.

Así sería bueno iniciar a partir de los formularios relevados, un análisis detallado de los procesos que involucran y disparan cada uno de estos formularios. Lo anterior se debería realizar bajo una visión global definida desde la SGP. Sería aconsejable en futuras consultorías iniciar un análisis funcional profundo involucrando todas las áreas y proyectos necesarios a fin de complementar un proyecto macro de modernización de las áreas tecnológicas bajo el ámbito de la SGP.

Enfoque Metodológico.

Luego de un análisis detallado de los formularios existentes, se desprende la necesidad de ahondar en la investigación y desarrollo de los mismos. Es beneficioso que a nivel de Gobierno se continúe con la creación de formularios y la evolución de los procesos asociados a la gestión de TI. Pero sería conveniente, y desde esta consultoría se lo entiende así, que se comience a analizar un enfoque global a toda la organización. Es decir que se amplíe el alcance del análisis a todos los procesos asociados a la gestión tecnológica. Este nuevo enfoque, integral, debería abarcar tanto sistemas como servicios TI, con el fin de poder avanzar hacia el modelado de la gestión integral asociada a las tecnologías de la información y las comunicaciones. El enfoque propuesto, se alinea perfectamente con las nuevas políticas de integración a nivel tecnológico que ha definido la gestión actual.

Se percibe una necesidad y decisión por parte de las áreas técnicas de comenzar con la documentación de procesos. La política actual de creación de nuevas áreas y la especialización de las mismas, conlleva a una interacción natural entre las mismas. Esto último producto de que numerosos procesos o circuitos necesariamente deben cruzar las fronteras de cada área, obligando a una interrelación fluida entre las mismas. Las áreas que se van conformando están constituidas por personal idóneo, que iniciará procesos de especialización y desarrollos específicos. Lo mencionado demandará procesos bien definidos y ágiles, producto de que complementariamente se disparará la demanda de los servicios TI en general.

Es importante también, comenzar a adoptar una metodología de modelado de procesos adecuada a este tipo de ámbitos, e incorporar paralelamente herramientas y tecnología acorde.

Análisis de los Formularios

Los formularios deberían evolucionar hacia el soporte completo de los procesos. Estos deberían ser redefinidos bajo premisas claras y alineadas con los objetivos globales del proyecto de Gobierno. Como ejemplo, el proceso de transformar formularios tradicionales o estáticos en formularios digitales autoeditables (ej. formato .pdf), se ve como un cambio necesario de realizar. De hecho, ya hay áreas que han comenzado a incursionar en esto. Lo anterior propuesto, agiliza notablemente los procesos que acompañan, y contribuye a reducir considerablemente los errores. Facilita la interacción y permite avanzar hacia la digitalización e informatización de los procedimientos asociados.

Si bien el formulario es una parte de los circuitos técnicos/administrativos el poder automatizarlos y/o digitalizarlos en las etapas iniciales de la reingeniería de los procesos que los contienen, es algo altamente beneficioso y aconsejable.

Un caso particular, en la digitalización de los formularios, es el caso de la Solicitud de una Cuenta de Correo Electrónico. Aquí el formulario se inicia en formato digital, pero por una cuestión de seguridad/autorización, se debe presentar en formato físico por la Mesa de Entradas y Salidas de la Secretaría de la Gestión Pública. Este formulario incorpora una sección de gestión dentro del mismo. Es decir, una vez

impreso y presentado por el solicitante, el formulario va registrando información propia de la gestión. Esto lo realiza a lo largo de la ejecución del proceso que lo define. Así, si bien esto es bueno para ordenar y regir el proceso, no es del todo deseable (ver Figura 10).

A modo de referencia se presenta más adelante en la Figura 11 el formulario F111 – “Solicitud de Usuario/Clave para acceso al Sistema Integrado S.I.I.F.” Este formulario se constituye en el principal a la hora de crear un usuario en el Sistema SIIF. Este es el sistema base, actualmente, para la integración de los restantes. Por esto, se debería centrar la atención sobre este formulario, y particularmente en el proceso que este formulario determina.

El conjunto de sistemas que está en desarrollo son el Sistema de Gestión de Documentos (SIGED), Sistema de Gestión de Obra Pública (SIGOP), Sistema del Instituto Provincial de la Vivienda (IPV), Sistema Integrado de Personas (SIP) y Sistema Integrado de Administración de Recursos Humanos (SIARH). Estos sistemas se integrarán en un futuro a la base del SIIF. Por lo cual se debería analizar fuertemente la interacción e integración de los procesos que involucran cada uno.

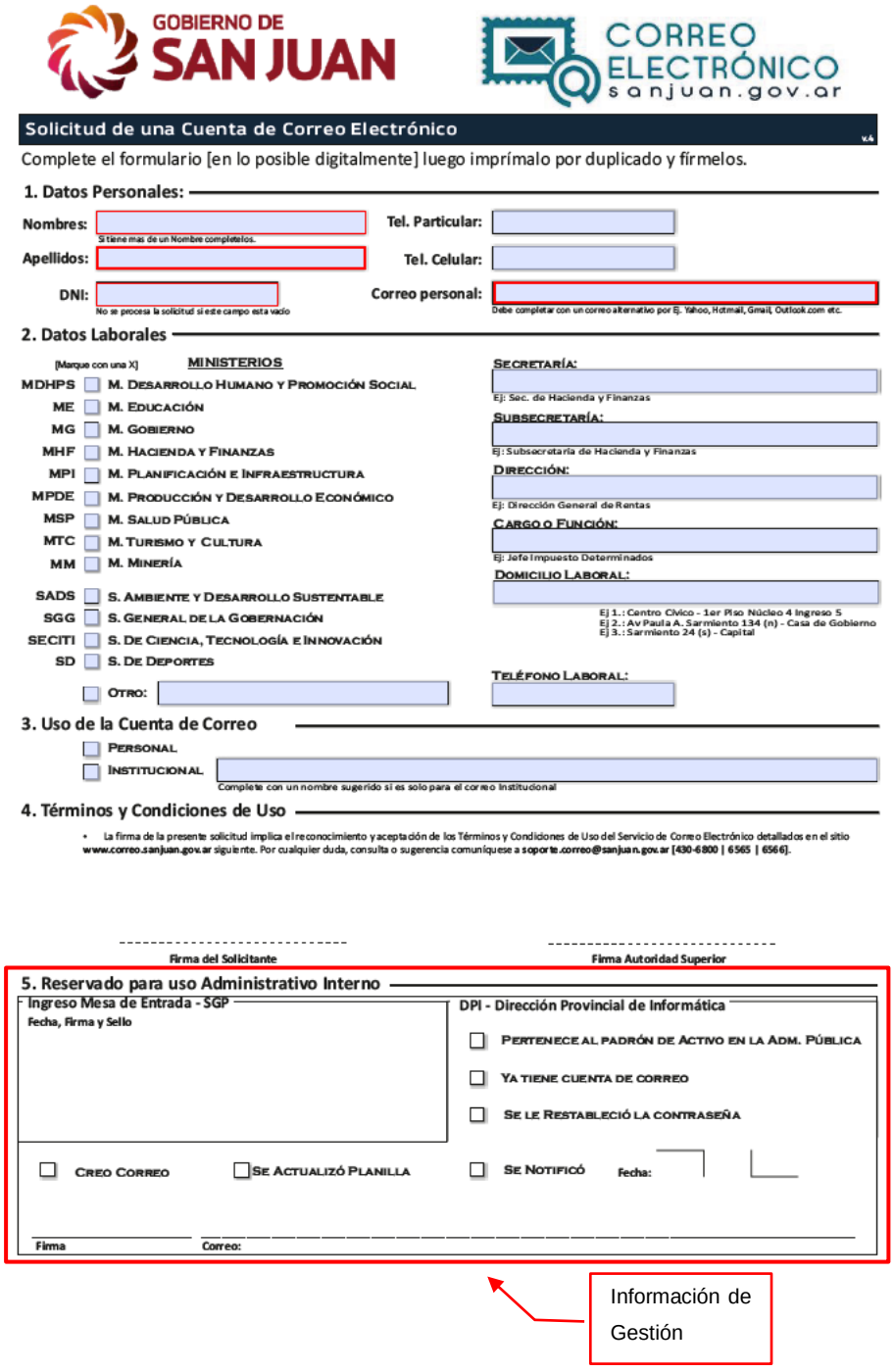


Figura 10 - Formulario de Solicitud de una Cuenta de Correo

F-111

GOBIERNO DE SAN JUAN

SOLICITUD DE USUARIO/CLAVE PARA ACCESO A SISTEMA INTEGRADO S.I.I.F.

Sr. Jefe Área Seguridad Informática

Por la presente solicito se le dé acceso como usuario del sistema integrado S.I.I.F. al siguiente agente, en compatibilidad con la función que desempeña **(MARQUE Y COMPLETE LO QUE CORRESPONDA)**:

	Usuario S.I.I.F.:			**ALTA**
	USUARIO DE RED:			**BAJA**
	OTRO SISTEMA:			**MODIFICACIÓN**

Datos Generales Del Usuario:

APELLIDO/S Y NOMBRE/S:		
ESTADO CIVIL:	**SEXO:**	**FECHA NACIMIENTO:**
TIPO / Nº DOCUMENTO:	**C.U.I.L. Nº:**	
DOMICILIO PARTICULAR: (CALLE/Nº/ORIENTACION) **LOCALIDAD:**	**DEPARTAMENTO:**	
TEL. CELULAR:	**TEL. LABORAL:**	**TEL. PARTICULAR:**
E-MAIL LABORAL:	**E- MAIL PERSONAL:**	

Dependencia Donde Presta Servicios El Usuario:

REPARTICION (Institución):
DEPENDENCIA FUNCIONAL (Actividad):
JEFE DE REPARTICION:
E-MAIL:

Describa la función que desempeña en el sistema integrado y a que módulos y/o perfil deberá acceder para realizarla:
FUNCION Y/O MODULOS QUE UTILIZARÁ:

Horario Habitual de Trabajo: **Horario Vespertino:**

IMPORTANTE: Si el Usuario realizara Tareas de Habilitado deberá acompañar indefectiblemente el Instrumento de Designación de la Función

Fecha de Entrega de la SOLICITUD: _____ / _____ / _____

Fecha de ALTA en el S.I: _____ / _____ / _____

DECLARO QUE LOS DATOS CONSIGNADOS EN ESTE FORMULARIO SON CORRECTOS Y COMPLETOS, SIN OMITIR DATO ALGUNO QUE DEBA CONTENER, SIENDO FIEL EXPRESIÓN DE LA VERDAD.

Firma del USUARIO	Firma y Sello del RESPONSABLE DEL ÁREA (Jefe Repartición)	Firma del Responsable del ALTA

Figura 11 – Solicitud de Usuario/Clave para acceso a Sistema Integrado SIIF

F-114

GOBIERNO DE SAN JUAN

SOLICITUD DE USUARIO/CLAVE PARA ACCESO A SISTEMA INTEGRADO S.I.GE.D.

Sr. Jefe Área Seguridad Informática

Por la presente solicito se le dé acceso como usuario del sistema integrado S.I.GE.D. al siguiente agente, en compatibilidad con la función que desempeña **(MARQUE Y COMPLETE LO QUE CORRESPONDA)**:

	Usuario S.I.GE.D.:			ALTA
	USUARIO DE RED:			BAJA
	OTRO SISTEMA:			MODIFICACIÓN

Datos Generales Del Usuario:

APELLIDO/S Y NOMBRE/S:		
ESTADO CIVIL:	SEXO:	FECHA NACIMIENTO:
TIPO / Nº DOCUMENTO:	C.U.I.L. Nº:	
DOMICILIO PARTICULAR: (CALLE/Nº/ORIENTACION)		
LOCALIDAD:	DEPARTAMENTO:	
TEL. CELULAR:	TEL. LABORAL:	TEL. PARTICULAR:
E-MAIL LABORAL:	E- MAIL PERSONAL:	

Dependencia Donde Presta Servicios El Usuario:

REPARTICION (Institución): DEPENDENCIA FUNCIONAL (Actividad): JEFE DE REPARTICION: E-MAIL:
Describa la función que desempeña en el sistema integrado y a que módulos y/o perfil deberá acceder para realizarla: FUNCION Y/O MODULOS QUE UTILIZARÁ:
Horario Habitual de Trabajo: Horario Vespertino:
IMPORTANTE: Si el Usuario realizara Tareas de Habilitado deberá acompañar indefectiblemente el Instrumento de Designación de la Función

Fecha de Entrega de la SOLICITUD: _____ / _____ / _____

Fecha de ALTA en el S.I.: _____ / _____ / _____

DECLARO QUE LOS DATOS CONSIGNADOS EN ESTE FORMULARIO SON CORRECTOS Y COMPLETOS, SIN OMITIR DATO ALGUNO QUE DEBA CONTENER, SIENDO FIEL EXPRESIÓN DE LA VERDAD.

Firma del USUARIO	Firma y Sello del RESPONSABLE DEL ÁREA (Jefe Repartición)	Firma del Responsable del ALTA

Figura 12 – Solicitud de Usuario/Clave para acceso a Sistema Integrado SIGED

Si se realiza un análisis visual rápido de los formularios de Solicitud de Correo Electrónico (Figura 10) y F111 (Figura 11), es fácil detectar la similitud en cuanto a tipo de información que cada uno de los formularios involucra. Luego el Formulario que se adoptó para el alta de usuarios del SIGED (Figura 12) es una copia casi exacta del F111. De lo anterior se desprende casi obligatoriamente iniciar un proceso de integración de estos formularios/procesos. Esto orientado a la unificación del proceso de alta de usuarios.

Formularios asociados al SIGED

El proceso de implementación del SIGED, conlleva un detallado relevamiento de la repartición u organismo en el cual se va a desplegar. En una primera etapa se trabajó en el análisis de formularios existentes asociados por los desarrolladores del Sistema. A continuación, se presentan a fin de obtener una primera impresión del alcance de los mismos.

Análisis Formulario F-114

El Formulario F-114 corresponde a: “Solicitud de Usuario/Clave para acceso al Sistema Integrado S.I.Ge.D.”. En la Figura 12, se presenta este formulario el cual fue analizado respecto a las secciones que lo componen, y su relación con los demás sistemas integrados y otros servicios de TI que pudieran ser necesarios de tener en consideración.

Las secciones que se identificaron son:

- Código del Formulario.
- Información de Seguridad e Infraestructura.
- Información Personal del Usuario.
- Información Laboral del Usuario.
- Información de Gestión del Formulario.
- Información de Seguridad.
- Versión del Formulario.

Código del Formulario

Es fundamental poder mantener y gestionar una codificación adecuada de toda la documentación asociada al SIGED y complementariamente de los otros Sistemas. Poder identificar unívocamente cada uno de los formularios es indispensable. Si bien parece básico lo aquí enunciado, es común que esta actividad se vaya diluyendo en el tiempo, y surjan versiones diferentes de diferentes autores. Se debería centralizar la codificación en una sola área. Y sería aconsejable centralizar también el mantenimiento y gestión de todos los formularios relacionados con los Sistemas Integrados. Igualmente sería interesante analizar la integración con los servicios de TI asociados. De esta forma, se logra dar un orden y cohesión global al proyecto en lo relacionado a la gestión de la documentación.

Información de Seguridad e Infraestructura.

Esta sección refiere a la gestión propiamente dicha del usuario en el entorno del Sistema SIGED. Este usuario es en realidad un usuario del Sistema SIIF, producto de la integración de ambos sistemas. Complementariamente se debe detallar la acción requerida al tratarse de un ABM de usuarios.

Ahora bien, un punto importante en esta sección es el campo que solicita “Usuario de Red”. Este usuario solicitado es el correspondiente a la red lógica sobre la cual ejecuta el sistema SIGED en este caso.

Información Personal del Usuario

Esta sección engloba información que es simple de entender y refiere a todos los datos asociados a una persona que se volverá usuario del Sistema. La información solicitada es bastante completa, y se la ha perfeccionado con el tiempo. La información personal del usuario es común a la mayoría de los sistemas, como así también de los Servicios TI. De aquí surge la necesidad de contar con un repositorio central con toda esta información y que no sea necesaria cargarla cada vez que la misma persona se vuelve usuaria de cada sistema o servicio.

Información Laboral del Usuario

La información laboral del usuario se la puede dividir en dos conjuntos:

1. Un conjunto que refiere al lugar, horario de trabajo e información sobre el superior responsable.
2. Un conjunto que refiere al aspecto funcional del Sistema respecto del usuario (“Función y/o módulos que utilizará”).

El primer conjunto de datos cumple con las mismas características de la Información Personal del Usuario. Esta se duplicará en todos los procesos de alta de usuarios de los distintos sistemas y servicios, ya que son propiedades del usuario.

Ahora bien, el segundo conjunto de información es el específico y particular del Sistema SIGED. Es lo distintivo, producto de la interacción del usuario con el sistema SIGED específicamente. Esta información no se comparte con ningún otro sistema o servicio. Quizás esta sea la única información propia o particular asociada al Sistema.

Información de Gestión del Formulario

Esta información es propia de la gestión del proceso. Particularmente en este caso del proceso de alta de un usuario.

Información de Seguridad

Esta información certifica que la información del formulario es válida. Tiene que ver con asegurar la legalidad y veracidad de la información. Es sumamente importante y fundamentalmente hay que asegurar su legalidad.

Versión del Formulario

Mantener el versionado de los Formularios y también de los procesos asociados es de suma importancia. Esto asegura una correcta evolución de las versiones. Consecuentemente, debe existir un correcto circuito de autorizaciones asociados.

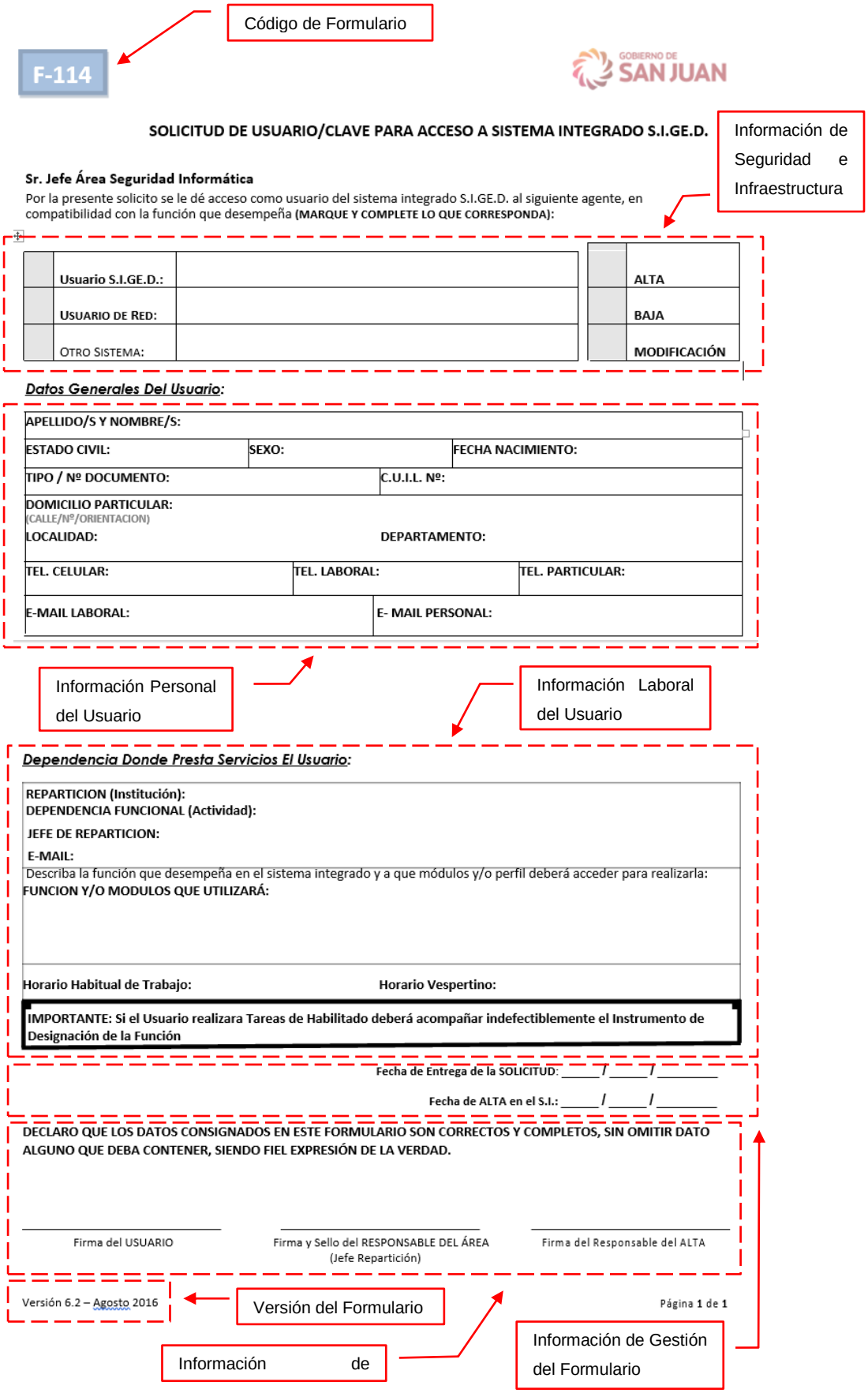


Figura 13 – Análisis de Datos del Formulario F-114

Relevamiento Sistema SIGED

Proceso de Relevamiento de Unidades Orgánicas

Al momento de decidir la incorporación de una nueva repartición o Unidad de Gobierno al Sistema SIGED, es necesario iniciar el proceso de alta de la misma. Este proceso engloba múltiples subprocesos, entre los cuales figura el relevamiento de lo que se denomina una Unidad Orgánica (en adelante UO). Es necesario relevar un gran volumen de información referente a los circuitos administrativos que abarcará la implementación del Sistema dentro de esa UO.

Para este relevamiento se han adaptado un conjunto de planillas o formularios que proveyó el equipo de desarrollo del Sistema. Es importante tener presente que el Sistema SIGED conforma un conjunto de sistemas bajo el concepto de Sistemas Integrados. Por lo cual toda acción a realizar a nivel de datos o configuraciones en el SIGED debe ser contextualizado a nivel general, y en particular a nivel del Sistema Integrado. En la actualidad el sistema madre o referencial, sería el Sistema SIIF.

A continuación, se presentan los formularios que se rediseñaron para llevar a cabo el relevamiento de cada una de las UO que se darán de alta al sistema.

Planilla de relevamiento:

1. Relevamiento de Unidades Orgánicas.
2. Relevamiento de Tipos de Documentos.
3. Relevamiento de Usuarios.
4. Relevamiento de Equipos.

Relevamiento de Unidades Orgánicas

MINISTERIO DE HACIENDA Y FINANZAS
SECRETARIA DE LA GESTIÓN PÚBLICA
DIRECCIÓN PROVINCIAL DE INFORMÁTICA

RELEVAMIENTO DE UNIDADES ORGÁNICAS

Institución: Secretaria Gestion Publica
Fecha: 02-09-2016
Referente:Norma Beatriz Gomez
Dígito de Identificación: SGP

Numero	Depende de	OFICINA (O UNIDADES ORGÁNICAS)	Es MESA DE ENTRADAS	GENERA DOCUMENTOS	PERMITE PASE EXTERNO
1		Sec. Gestion Publica	no	no	No
2	1	Subsec. Gestion Publica	no	no	No
3	1	Asesores	no	no	No
4	1	Programas Calidad	no	no	No
5	1	Prog. Cond. A la Defensiva	no	no	No

Figura 14 – Planilla de Relevamiento de Unidades Orgánicas

En el SIGED se denomina cada una de las áreas de la organización a modelar como Unidad Orgánica. Es decir, la mínima agrupación de agentes y sub áreas que serán administradas como una unidad. Es decir, que es la mínima división organizacional que puede recibir parametrizaciones particulares respecto del resto. Una Unidad Orgánica se debería correlacionar a nivel del organigrama con un área o subdivisión que pertenece a una Institución de Gobierno. Y una Institución de Gobierno podría ser el equivalente de una Dirección. Lo anterior es solo a modo referencial, pero es una práctica que se adecúa a la filosofía del Sistema. Si bien no es obligatorio, sería lo que aconseja el equipo Funcional del Sistema. Resumiendo, un conjunto de Unidades Organizacionales conforma una Institución.

Para el relevamiento de las UO, se definió la Planilla de “Relevamiento de Unidades Orgánicas”, la cual se presenta en la Figura 14. Esta planilla, una vez completada, será la base del proceso de alta en forma manual en los distintos ambientes de trabajo como son desarrollo, capacitación y/o producción. La misma contiene un encabezado donde figura la identificación de la Institución, La fecha del relevamiento, el responsable de hacerlo, y el Dígito de Identificación de la misma.

Análisis de las columnas de la planilla

La columna **[Número]** determina el orden secuencial en que fueron cargadas las UO en la planilla, pero a su vez determina la identificación unívoca de cada una que fue relevada. El orden debe ser correlativo ascendente, iniciando en 1. Luego la columna **[Depende de]** determina la dependencia funcional entre las UOs relevadas en la planilla. La finalidad de esta columna es poder plasmar el organigrama de la institución en el relevamiento. Es decir que, en esta columna, para cada UO debe figurar el Número de orden de la UO de la cual depende. A modo de ejemplo, en la planilla presentada en la Figura 4, la UO “Asesores” (fila 19) posee el valor “1” en la columna **[Depende de]**. Esto indica que depende de la UO “Sec. Gestión Pública” que posee el valor “1” en la columna **[Número]**. Una vez completado el relevamiento de estas dos columnas es posible, mediante herramientas de modelado, realizar el diagrama gráfico del organigrama de la Institución en forma dinámica y automática a partir de la Planilla de Relevamiento de Unidades Orgánicas.

Luego la columna **[Oficina]** representa el nombre de la UO que se está definiendo.

La columna **[Es Mesa de Entradas]** indica si esa oficina o UO posee la capacidad de iniciar un documento, como por ejemplo puede ser un Expediente. Sería la función típica de una Mesa de Entradas y Salidas de la AP.

La columna **[Genera Documento]** indica si esa oficina tiene la capacidad de generar un documento.

La columna **[Permite Pase Externo]** indica si esta oficina posee la capacidad de enviar documentos a UOs externas a la Institución que ella pertenece. Esta condición de enviar documentos o hacer pases a UOs externas, es propiedad por defecto de las Mesas de Entradas y Salidas. Mediante esta configuración, se le puede asignar esta propiedad a una UO en particular si la Institución así lo determinara. En esto es muy importante entender y respectar la forma de trabajo de cada una de las organizaciones modeladas. Pero sin duda alguna, sería muy conveniente comenzar a elaborar y discutir criterios que sean aplicables en forma transversal todas las reparticiones de la APP.

Relevamiento de Tipos de Documentos

GOBIERNO DE SAN JUAN

MINISTERIO DE HACIENDA Y FINANZAS
SECRETARIA DE LA GESTIÓN PÚBLICA
DIRECCIÓN PROVINCIAL DE INFORMÁTICA

RELEVAMIENTO TIPO DE DOCUMENTOS

Institución:
Fecha:
Referente:

Tipo de Documento	Datos Específicos	Dato Específico Obligatorio	Dato Específico Imprimible
Nota	*Reparticion Iniciador Extracto*	*SI*	*SI*
Expedientes	Reparticion Iniciador Extracto	si	si
Oficios	Reparticion Iniciador Extracto	si	si

Figura 15 – Planilla de Relevamiento de Tipo de Documento

El SIGED posee la capacidad de definir los Tipos de Documentos, es decir qué tipo de documentación específica y claramente definida es posible de generar y gestionar a nivel de Institución. Para esta definición se emplea la Planilla de "Relevamiento de Tipo de Documentos" que se muestra en la Figura 15.

El ejemplo presentado en la Figura 15, corresponde al relevamiento de la Institución Secretaría de la Gestión Pública.

Análisis de las columnas de la planilla

En el encabezado de la planilla figuran los siguientes datos: **[Institución]** que es el nombre de la Institución relevada, es decir que define el ámbito de alcance de los tipos de documentos que se definen en el cuerpo de la planilla. El Campo **[Fecha]** que indica la fecha en que fue realizado el relevamiento. Y el dato **[Referente]** que indica quien es la persona responsable de las definiciones que involucra la planilla.

El cuerpo de la planilla posee los siguientes datos: **[Tipo de Documento]** que indica el nombre del documento que se está definiendo. **[Datos Específicos]** indica el conjunto de datos específicos que debe incluir el documento además de los básicos estándares del mismo. Estos datos básicos se definen dentro del ámbito de la Institución. La columna **[Dato Específico Obligatorio]** indica si el dato indicado en la columna anterior es de carácter obligatorio o no. La columna **[Datos Específico Imprimible]** indica si es necesario que el dató indicado en la columna **[Datos Específicos]** es necesario que aparezca en la impresión del documento.

Relevamiento de Usuarios

GOBIERNO DE SAN JUAN

MINISTERIO DE HACIENDA Y FINANZAS
SECRETARIA DE LA GESTIÓN PÚBLICA
DIRECCIÓN PROVINCIAL DE INFORMÁTICA

RELEVAMIENTO DE USUARIOS

Institución: Secretaria GestionPublica
Fecha: 02-09-2016
Referente: Norma Beatriz Gomez

APELLIDO	NOMBRES	DNI	OFICINA (UNIDAD ORGÁNICA)	PERMITE CONSULTAS DE DOCUMENTOS	GENERA DOCUMENTOS	RECIBE Y ENVÍA DOCUMENTOS
Rupcic	Andres	25.319.873	Sec. Gestion Publica	No	No	Si
Quijano	Juan	25.991.737	Subsec. Gestion Publica	No	No	Si
Gomez	*Norma Beatriz*	16.931.726	Mesa de Entradas	No	Si	Si
Maldonado	Ruben Emilio	13.497.128	Mesa de Entradas	No	Si	Si
Murciano	Duilio	16.332.260	Mesa de Entradas	No	No	Si
Rius	Natacha	13.107.477	Despacho	No	Si	Si
Sassul	Eduardo	14.474.874	Direccion Administrativa	No	No	Si
Camino	Ruben	17.313.597	Asesoria Legal	No	No	Si
Ramirez	Eugenia	14.972.559	Compras y Contable	No	No	Si

Figura 16 – Planilla de Relevamiento de Usuarios

Un relevamiento importante es el de usuarios del sistema, en este caso del SIGED. Cada uno de los agentes de la Institución que necesite interactuar con el sistema, necesita tener creado un usuario y su correspondiente parametrización. Con la Planilla de Relevamiento de Usuarios (Figura 16), se lleva a cabo el relevamiento de usuarios.

Análisis de las columnas de la planilla

En el encabezado de la planilla figuran los siguientes datos: **[Institución]** que es el nombre de la Institución relevada, es decir que define la institución a la que deben pertenecer los usuarios para ser incluidos en la planilla. El Campo **[Fecha]** que indica la fecha en que fue realizado el relevamiento. Y el dato **[Referente]** que indica quien es la persona responsable de las definiciones que involucra la planilla.

El cuerpo de la planilla contiene los siguientes campos:

[APELLIDO], **[NOMBRE]** y **[DNI]** refieren a datos particulares y puntuales de cada uno de los usuarios del Sistema. La columna **[OFICINA]** indica la oficina o UO a la que pertenece el usuario. La columna **[PERMITE CONSULTA DE DOCUMENTOS]** refiere a la posibilidad por parte del usuario a acceder al módulo de consulta de documentos. La columna **[GENERA DOCUMENTOS]** refiere a si el usuario posee derechos de generación de documentos. La columna **[RECIBE Y ENVIA DOCUMENTOS]** indica si el usuario tiene permisos para recibir y enviar documentos.

Relevamiento de Equipos

GOBIERNO DE SAN JUAN

MINISTERIO DE HACIENDA Y FINANZAS
SECRETARIA DE LA GESTIÓN PÚBLICA
DIRECCIÓN PROVINCIAL DE INFORMÁTICA

RELEVAMIENTO DE EQUIPOS

Institución: Secretaria Gestion Publica
Fecha:
Referente: Norma Beatriz Gomez

APELLIDO	NOMBRES	OFICINA (UNIDAD ORGÁNICA)	Identificación PC	IMPRESORA	LECTOR C. BARRA	S.O.	Navegador Web	ACCESO AL SIIF	RED (IP)
Rupcic	Andres	Sec. Gestion Publica							
Quijano	Juan	Subsec. Gestion Publica							
Gomez	Norma Beatriz	Mesa de Entrada							
Maldonado	Ruben Emilio	Mesa de Entrada							
Gomez	Carlos	Mesa de Entradas							
Murciano	Duilio	Mesa de Entrada							
Rius	Natacha	Despacho							
Sassul	Eduardo	Direccion Administrativa							

Figura 17 – Planilla de Relevamiento de Equipos

La planilla de “Relevamiento de Equipos” (Figura 17) fue diseñada para permitir conocer el estado del equipamiento informático que posee la Institución que está siendo relevada respecto al uso del Sistema SIGED. Es necesarios relevar c/u de las estaciones de trabajo donde se ejecutará el Sistema, con el fin de prever que este funcione adecuadamente. Los datos solicitados son estrictamente técnicos, escapan al ámbito de estudio por parte de esta consultoría. De todos modos, se refieren a características técnicas de la PCs que usa cada uno de los usuarios del Sistema. Lo relevante es que debe cargarse el **[APELLIDO]**, **[NOMBRE]** de cada usuario, y la **[OFICINA]** (UO) en la que trabaja el agente.

Consideraciones en el Alta de Usuarios del SIGED

El Formulario F-114 (Figura 13), sería el empleado para realizar el alta de un usuario al Sistema SIGED. Si bien es un proceso ya consolidado, presenta un inconveniente. Esto desde el punto de vista que es la evolución del proceso de alta del SIIF. A la hora de dar de alta una Institución, seguramente será necesario también dar de alta un conjunto grande de usuarios en forma simultánea. Esta realidad se presentará en numerosas ocasiones en los próximos meses, producto de la expansión y masificación que experimentará el SIGED. Lo anterior disparado por la política impuesta desde la SGP de estandarizar y transversalizar el Sistema a todo el ámbito de la APP.

Por lo enunciado es que se propone iniciar el diseño de un nuevo formulario que permita el alta masiva y simultanea de una cantidad importante de usuarios al Sistema y que involucre un solo proceso de autorización. Esto debería considerarse a nivel de Institución.

Modelado de Procesos

A continuación, se propone el modelado de procesos, mediante el empleo de una metodología simple cercana a BPM. La idea subyacente, es iniciar a la organización, en este caso el Gobierno de San Juan en la mejora y gestión de procesos. Imponer una nueva forma de entender los objetivos y metas de la Gestión Pública.

Así se presupone la idea de que se ve el rol y las funciones de la administración pública como un conjunto de procesos y es necesario iniciar la mejora de los mismos.

La idea es tratar de orientarse hacia la administración de procesos de negocio, (BPM – en ingles *Business Process Management*), que es una disciplina que involucra una combinación de modelado, automatización, ejecución, control, medición y optimización de los flujos de actividad de negocios, en apoyo de objetivos de la empresa, que abarcan sistemas, empleados, clientes y socios dentro y fuera de los límites de la empresa".

Este concepto o en un sentido más amplio, esta “disciplina” si bien proviene del mundo empresarial, es perfectamente aplicable a los entornos de Administración Pública para mejorar en todas las dimensiones los procesos que conforman la actividad.

Desde esta consultoría, se considera fundamental avanzar en el entendimiento de los procesos que se desenvuelven dentro del ámbito de Gobierno, y fundamentalmente iniciar el proceso de mejora de los mismos. Es básico entender los procesos en el contexto de actividades interrelacionadas holísticamente que cooperan para cumplir un objetivo organizacional. Esta es la diferencia clave de una visión funcional de las actividades gubernamentales donde cada función puede ser optimizada independientemente de las otras. En un sistema complejo como es la gestión pública, es conocido que la optimización local o individual de parte del sistema rara vez conducirá a buenos resultados generales. Se deben considerar las métricas de todo el sistema al evaluar un proceso específico.

Proceso

El proceso central propuesto se basa en una metodología de diagramas y documentos. A continuación, se irá explicando la forma de desarrollarlo.

Un aspecto fundamental es la identificación de un responsable o coordinador general para cada uno de los procesos relevados. Esto es esencial, ya que normalmente los mismos suelen desarrollarse a través de distintas áreas,

departamentos, inclusive reparticiones. Lo que se conoce como procesos *cross*. Es recomendable, que un agente entienda claramente el propósito del proceso, la finalidad y todo lo involucrado con el desarrollo del mismo. Y fundamentalmente el alcance. Quizás en algunos casos, será necesaria la coordinación entre dos responsables en el caso que el proceso sea muy extenso. Pero, en base a la experiencia, normalmente es suficiente con un solo agente, el cual pude englobar la totalidad del alcance del mismo.

Este coordinador, es recomendable que sea una persona con el conocimiento claro y global de lo que el proceso involucra. Necesariamente no debe ser un experto en cada una de las actividades involucradas, simplemente deberá contar con el conocimiento general, y fundamentalmente tener capacidades de coordinación y liderazgo para poder evolucionar el proceso. Una buena elección de este tipo de personal, determinan fuertemente los proyectos de modelado y rediseño de procesos dentro de una organización.

A continuación, se detallarán un conjunto de herramientas y recomendaciones, que son la base de una metodología básica de modelado de procesos propuesta. En la medida que se vaya desarrollando la misma, se irán enunciado acuerdos y recomendaciones que completarán la misma.

Diagrama de Actividades

El componente central es un simple diagrama, ya mencionado, como es el Diagrama de Actividades. Este diagrama forma parte del Lenguaje de Modelado Unificado (UML). En la Figura 18 se presenta el Diagrama de Actividades correspondiente al Proceso “Alta de Usuario Sistema SIIF”. Se lo presenta en esta instancia a fin de poder visualizarlo y analizarlo gráficamente. Más adelante se lo presentará en forma más detallada.

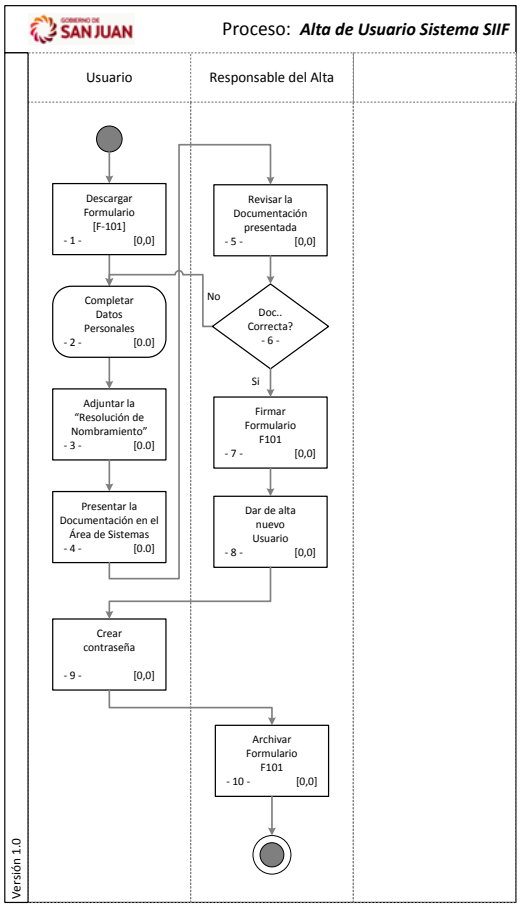


Figura 18 – Diagrama de Actividades.

Este diagrama posee la particularidad de una simpleza notable, y estar basado en una herramienta de documentación tradicional y muy conocida como es el "Diagrama de Flujo". Es un modelado gráfico que se entiende casi naturalmente, y bastante conocido en diversas ciencias del conocimiento asociadas a la gestión y la organización.

Así, es claro interpretar que existe un camino o flujo de información, el cual está determinado por las flechas, las cuales van uniendo cada una de las unidades funcionales o divisiones del trabajo, que representan las actividades.

En el circuito administrativo, que determina el flujo correspondiente, se encuentran rombos, los cuales tienen la función de definir las decisiones involucradas en el circuito modelado. Ante determinadas condiciones, será necesario desarrollar un determinado conjunto de actividades.

Complementariamente, existen otras numerosas figuras que van complementando el diagrama.

Otro de los componentes fundamentales del Diagrama de Actividades, son las denominadas “calles” o “roles” intervinientes en el proceso. Estas son generalmente las divisiones verticales que se observan, y corresponden a los “roles” que participan en el proceso.

En el ejemplo presentado, podemos observar 2 calles. Las cuales son: “Usuario”, “Responsable de Alta”. Es decir que todas las actividades que se ubican verticalmente dentro de la calle denominada “Usuario”, son ejecutadas y responsabilidad del conjunto de agentes que desempeñan ese rol. De esta forma se va modelando el proceso identificando las unidades de trabajo indivisibles (las actividades) y sus ejecutores.

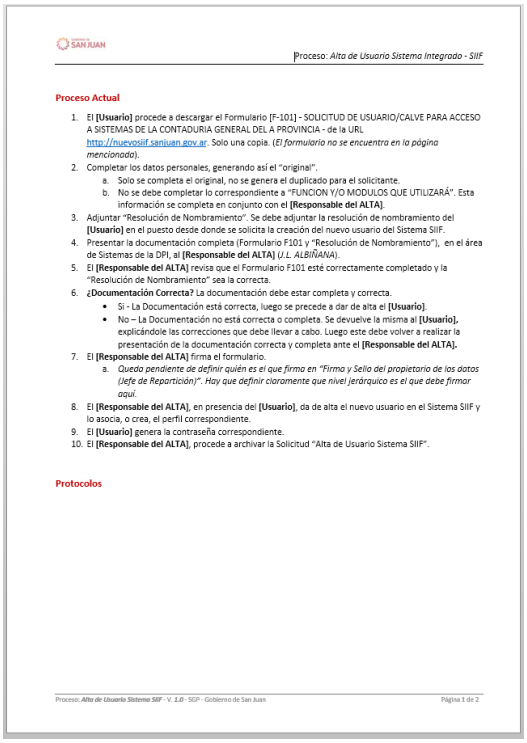
De este tipo de gráficos surgen numerosos análisis muy detallados, por cierto. A modo de ejemplo se cita, por ejemplo, que es posible visualizar que roles poseen mayor carga de unidades de trabajo que otras. Esto a través de contabilizar la cantidad de actividades que cada calle involucra. De aquí, es posible analizar que, ante un planteo de necesidad de optimización del proceso, nace naturalmente la opción de poner especial énfasis en asignar un mayor número de agentes a las calles o roles más cargadas. O quizás subdividir esa área en otras áreas más pequeñas. Las cuales absorban subconjuntos de actividades a fin de optimizar el proceso.

También es posible representarán otros posibles enfoques de optimización de procesos que surgen de la aplicación de los Diagramas de Actividades, como por ejemplo la inclusión de variables como pueden ser el tiempo o costo.

Detalle de Actividades

El Detalle de Actividades (documento de texto o formato similar), el cual tiene por finalidad básica la de complementar y describir cada una de las actividades que conforman el proceso en su totalidad representado por el Diagrama de Actividades.

Como ya fue mencionado, las actividades se representan mediante la figura del rectángulo.



SAN JUAN

Proceso: *Alta de Usuario Sistema Integrado - SIIF*

Proceso Actual

1. El **[Usuario]** procede a descargar el Formulario [F-101] - SOLICITUD DE USUARIO/CALVE PARA ACCESO A SISTEMAS DE LA CONTADURÍA GENERAL DEL A PROVINCIA - de la URL http://nuevosiif.sanjuan.gov.ar. Solo una copia. (*El formulario no se encuentra en la página mencionada*).
2. Completar los datos personales, generando así el "original".
   a. Solo se completa el original, no se genera el duplicado para el solicitante.
   b. No se debe completar lo correspondiente a "FUNCION Y/O MODULOS QUE UTILIZARÁ". Esta información se completa en conjunto con el **[Responsable del ALTA]**.
3. Adjuntar "Resolución de Nombramiento". Se debe adjuntar la resolución de nombramiento del **[Usuario]** en el puesto desde donde se solicita la creación del nuevo usuario del Sistema SIIF.
4. Presentar la documentación completa (Formulario F101 y "Resolución de Nombramiento"), en el área de Sistemas de la DPI, al **[Responsable del ALTA]** (*J.L. ALBIÑANA*).
5. El **[Responsable del ALTA]** revisa que el Formulario F101 esté correctamente completado y la "Resolución de Nombramiento" sea la correcta.
6. **¿Documentación Correcta?** La documentación debe estar completa y correcta.
   - Si - La Documentación está correcta, luego se precede a dar de alta el **[Usuario]**.
   - No – La Documentación no está correcta o completa. Se devuelve la misma al **[Usuario],** explicándole las correcciones que debe llevar a cabo. Luego este debe volver a realizar la presentación de la documentación correcta y completa ante el **[Responsable del ALTA].**
7. El **[Responsable del ALTA]** firma el formulario.
   a. *Queda pendiente de definir quién es el que firma en "Firma y Sello del propietario de los datos (Jefe de Repartición)". Hay que definir claramente que nivel jerárquico es el que debe firmar aquí.*
8. El **[Responsable del ALTA]**, en presencia del **[Usuario]**, da de alta el nuevo usuario en el Sistema SIIF y lo asocia, o crea, el perfil correspondiente.
9. El **[Usuario]** genera la contraseña correspondiente.
10. El **[Responsable del ALTA]**, procede a archivar la Solicitud "Alta de Usuario Sistema SIIF".

Protocolos

Proceso: *Alta de Usuario Sistema SIIF* - V. *1.0* - SGP - Gobierno de San Juan Página 1 de 2

Figura 19 – Detalle de Actividades complementarias al Diagrama de Actividades.

El Detalle de Actividades, el cual complementa al Diagrama de Actividades, tiene por finalidad principal, la de presentar una vista para el entendimiento fino y detallado del proceso y en especial de cada una de las actividades. Es decir, se pueden detallar rigurosamente cada una de las actividades que conforman el proceso, como así también las condiciones, y determinantes que participan, o son necesarias a la hora de tomar decisiones en la ejecución y seguimiento del flujo asociado al proceso.

Cada una de las actividades se identifica con un número, el cual da un orden correlativo y ascendente. Este orden no responde a un criterio riguroso, simplemente pretende acompañar el flujo natural secuencial que poseen naturalmente los procesos. Lo importante es la condición de unicidad en la identificación de cada una de las actividades. Debe ser entendido y empleado como una calve única de cada actividad

Este documento puede ser redactado en cualquier herramienta de documentación textual. Y tiene inmersa la simplicidad de la redacción con la posibilidad de un nivel elevado de detalle. Es importante aquí comprender y aplicar ciertos criterios de redacción simple, directa, con oraciones cortas y bien construidas, dándole especial énfasis al empleo de los verbos correspondientes.

Complementariamente, se propone trabajar con la definición de protocolos. Los cuales se detallarán en el siguiente punto. Dichos protocolos, deben ser también identificados con el mismo número que se asignó a la actividad que lo involucra. Así cada uno de los protocolos deber estar asociado a una actividad determinada. Esto facilita la identificación del mismo, y especialmente define el responsable de la aplicación del mismo.

Protocolos

Complementariamente, se incorpora un objeto de documentación muy valioso, como es el “protocolo”. Un protocolo puede ser entendido como un reglamento o una serie de instrucciones que se fijan o se acuerdan por convenio. Partiendo de este significado, es posible emplear la noción en diferentes contextos. En nuestro caso un protocolo será un documento (formulario o planilla), o una normativa que establece detalladamente cómo se debe actuar, o que realizar concretamente en ciertos procedimientos o situaciones. De este modo, recopila y expresa conductas, acciones y técnicas que se consideran adecuadas u obligatorias ante ciertas situaciones.

El protocolo, tiene entre sus múltiples ventajas, la de facilitar el apego a la norma legal. Elimina concretamente la duda o la indefinición, ante determinadas situaciones o procedimientos. La idea es que muestre con claridad los datos necesarios y obligatorios a requerir, u completar.

Los protocolos pueden poseer diversos formatos, todo atendiendo a la cultura y costumbres de la organización modelada. Aquí también, hay que considerar las herramientas que se poseen. Ya santos sistemas, formularios electrónicos, documentación en papel, gestores de contenidos, por nombrar algunos.

Gestión de Documentos

La 3° sección del documento “Detalle de Actividades”, corresponde a la Gestión de Documentos. Aquí simplemente se debe ir documentando todo Cambio, Revisión y Aprobación que se ejecuta mientras se lleva a cabo el diseño y modelado del proceso. Es bueno aclarar que el “Diagrama de Actividades” y el “Detalle de Actividades” son documentos fuertemente relacionados. Es decir que no pueden ser trabajados ni evolucionados en forma separada. Por lo cual esta sección de la “Gestión de Documentos” debe referirse a ambos.

A continuación, se presenta la Figura 20 que presenta la sección Gestión de Documentos para el proceso “Alta de Usuario Sistema SIIF”.

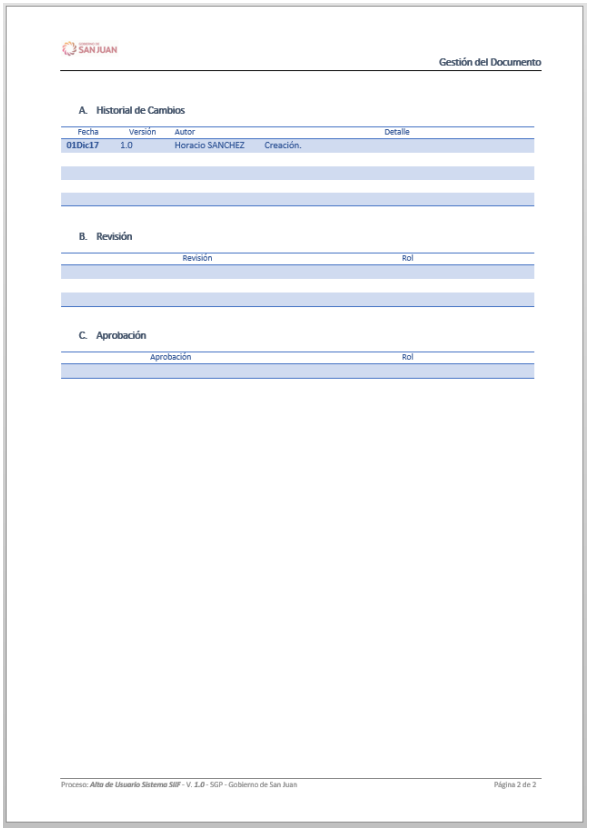
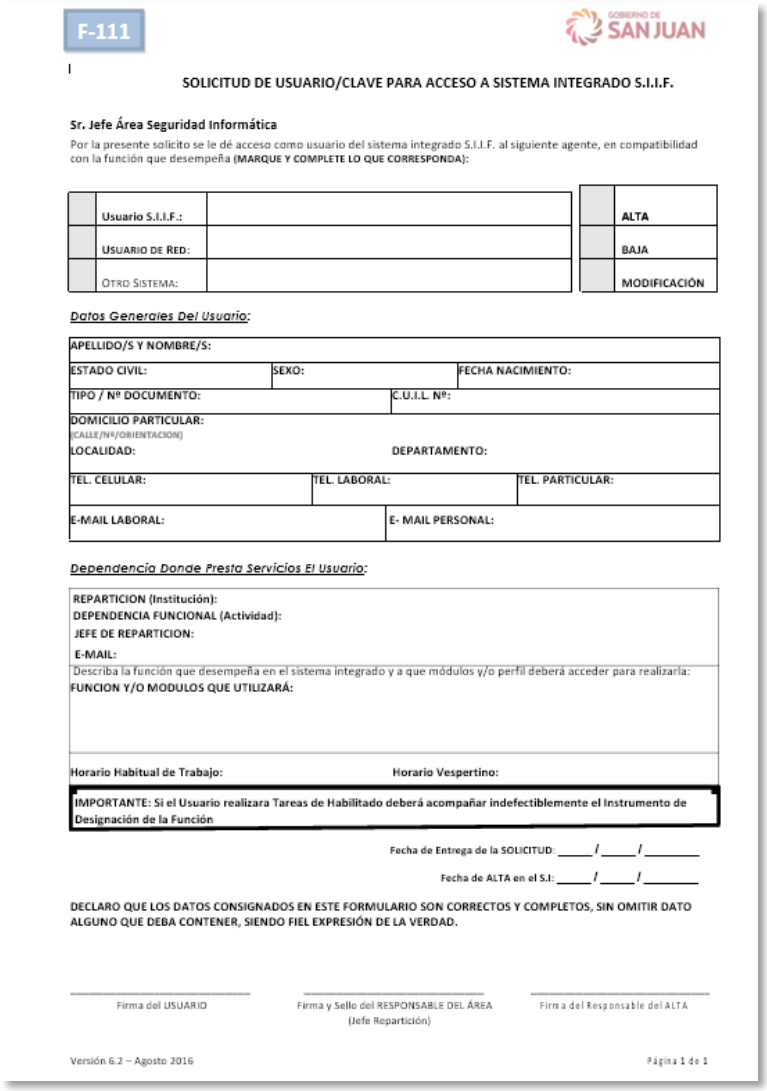


Figura 20 – Hoja de Gestión de Documentos.

Relevamiento Inicial

En base a los conceptos planteados, se comenzó a trabajar en la primera fase que corresponde al modelado de procesos. El primer proceso sobre el cual se comenzó a trabajar es el del “Alta de Usuario Sistema SIIF”. Este, corresponde al proceso que se sigue actualmente para proceder a dar de alta a un usuario nuevo en el Sistema SIIF actualmente. Es el empleado por el Área de Sistemas de la SGP y tiene como documento base el Formulario F-111, ya presentado en el primero informe de la presente consultoría. A continuación, se presenta una imagen de dicho formulario.



F-111

GOBIERNO DE SAN JUAN

SOLICITUD DE USUARIO/CLAVE PARA ACCESO A SISTEMA INTEGRADO S.I.I.F.

Sr. Jefe Área Seguridad Informática

Por la presente solicito se le dé acceso como usuario del sistema integrado S.I.I.F. al siguiente agente, en compatibilidad con la función que desempeña **(MARQUE Y COMPLETE LO QUE CORRESPONDA):**

	Usuario S.I.I.F.:			ALTA
	USUARIO DE RED:			BAJA
	OTRO SISTEMA:			MODIFICACIÓN

Datos Generales Del Usuario:

APELLIDO/S Y NOMBRE/S:		
ESTADO CIVIL:	SEXO:	FECHA NACIMIENTO:
TIPO / Nº DOCUMENTO:	C.U.I.L. Nº:	
DOMICILIO PARTICULAR: (CALLE/Nº/ORIENTACION)		
LOCALIDAD:	DEPARTAMENTO:	
TEL. CELULAR:	TEL. LABORAL:	TEL. PARTICULAR:
E-MAIL LABORAL:	E- MAIL PERSONAL:	

Dependencia Donde Presta Servicios El Usuario:

REPARTICION (Institución):
DEPENDENCIA FUNCIONAL (Actividad):
JEFE DE REPARTICION:
E-MAIL:

Describa la función que desempeña en el sistema integrado y a que módulos y/o perfil deberá acceder para realizarla:
FUNCION Y/O MODULOS QUE UTILIZARÁ:

Horario Habitual de Trabajo: Horario Vespertino:

IMPORTANTE: Si el Usuario realizara Tareas de Habilitado deberá acompañar indefectiblemente el Instrumento de Designación de la Función

Fecha de Entrega de la SOLICITUD: _____/_____/_____

Fecha de ALTA en el S.I: _____/_____/_____

DECLARO QUE LOS DATOS CONSIGNADOS EN ESTE FORMULARIO SON CORRECTOS Y COMPLETOS, SIN OMITIR DATO ALGUNO QUE DEBA CONTENER, SIENDO FIEL EXPRESIÓN DE LA VERDAD.

Firma del USUARIO | Firma y Sello del RESPONSABLE DEL ÁREA (Jefe Repartición) | Firma del Responsable del ALTA

Versión 6.2 – Agosto 2016 Página 1 de 1

Figura 21 – Formulario F-111 – Alta Usuario Sistema SIIF

Este formulario ha sido desarrollado inicialmente y evolucionado posteriormente en forma continua por parte de personal de la Contaduría General de la Provincia. En la actualidad lo mantiene personal de la Secretaría de la Gestión Pública. Es importante analizar varios aspectos sobre le mismo, en especial el tipo de información que contiene. El concepto de proceso es bastante más amplio, y corresponde a una totalidad funcional y a una integración con los restantes sistemas y servicios TI respecto del alta de un usuario. Todo lo anterior bajo el enfoque de integración propuesto por la SGP. Así planteada la metodología se propone comenzar a trabajar en futuras consultorías en el rediseño o reingeniería de este proceso como de los relacionados.

A continuación, se presentan tres Figuras (22, 23 y 24) que muestran el modelado del proceso actual.

Nota: *El presente proceso no posee ningún protocolo definido, por lo cual esa sección está vacía. Solo se deja la referencia en el Detalle de Actividades a fin de ejemplificarlo mejor*.

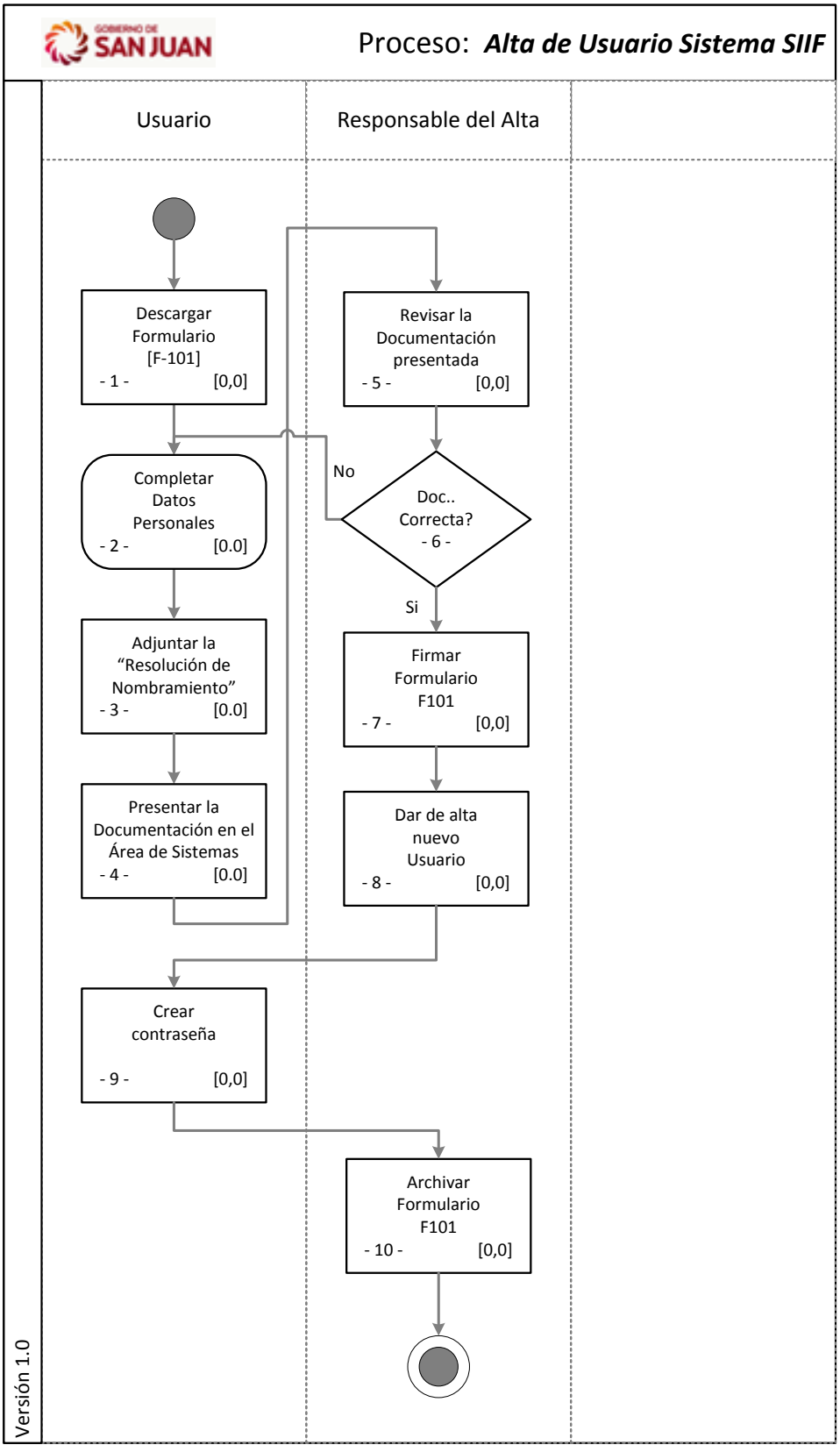


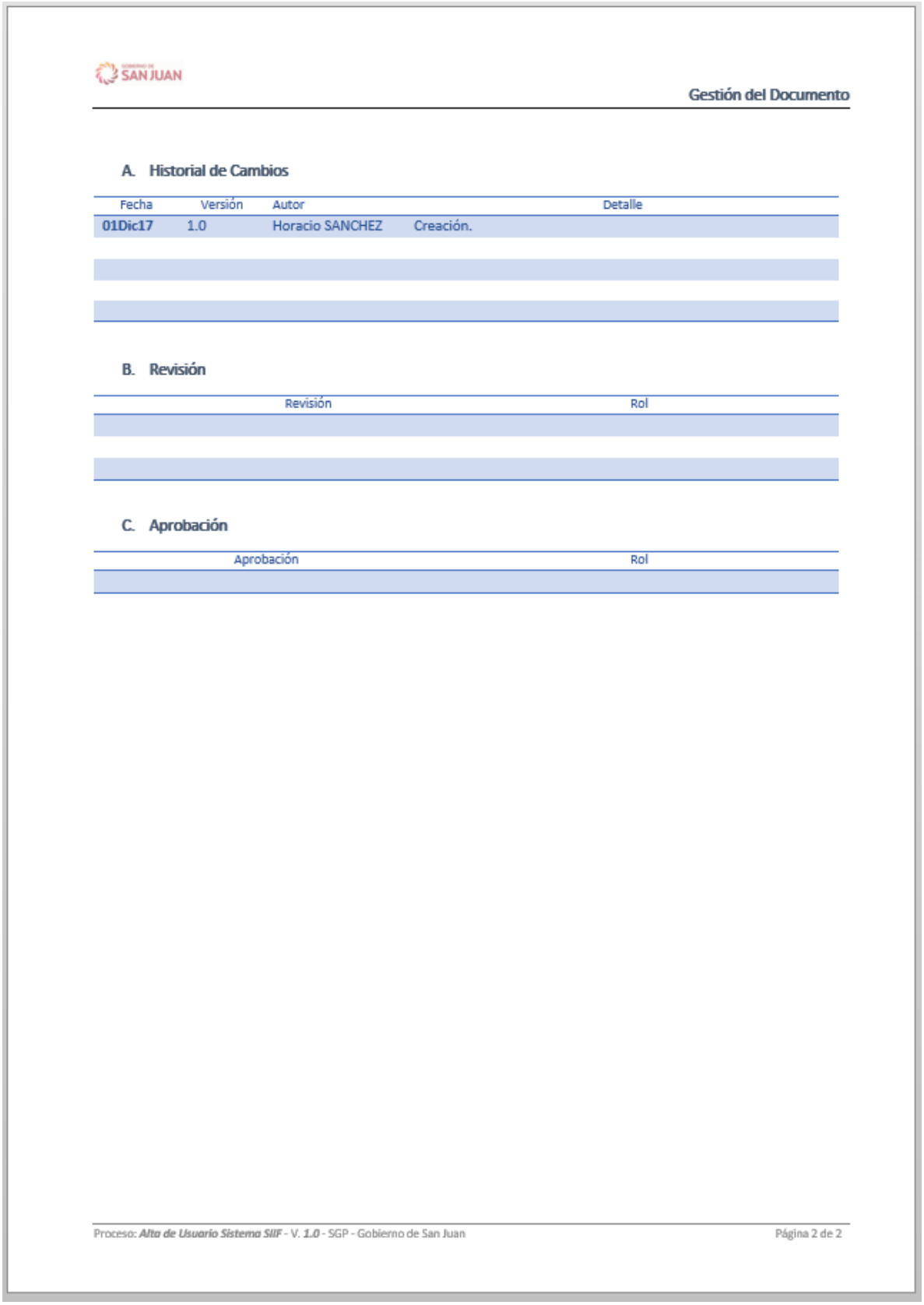
Figura 22 – Diagrama de Actividades del Proceso: *Alta de Usuario Sistema SIIF.*

Proceso Actual

1. El **[Usuario]** procede a descargar el Formulario [F-101] - SOLICITUD DE USUARIO/CALVE PARA ACCESO A SISTEMAS DE LA CONTADURIA GENERAL DEL A PROVINCIA - de la URL http://nuevosiif.sanjuan.gov.ar. Solo una copia. (*El formulario no se encuentra en la página mencionada*).
2. Completar los datos personales, generando así el "original".
    a. Solo se completa el original, no se genera el duplicado para el solicitante.
    b. No se debe completar lo correspondiente a "FUNCION Y/O MODULOS QUE UTILIZARÁ". Esta información se completa en conjunto con el **[Responsable del ALTA]**.
3. Adjuntar "Resolución de Nombramiento". Se debe adjuntar la resolución de nombramiento del **[Usuario]** en el puesto desde donde se solicita la creación del nuevo usuario del Sistema SIIF.
4. Presentar la documentación completa (Formulario F101 y "Resolución de Nombramiento"), en el área de Sistemas de la DPI, al **[Responsable del ALTA]** (*J.L. ALBIÑANA*).
5. El **[Responsable del ALTA]** revisa que el Formulario F101 esté correctamente completado y la "Resolución de Nombramiento" sea la correcta.
6. **¿Documentación Correcta?** La documentación debe estar completa y correcta.
    - Si - La Documentación está correcta, luego se precede a dar de alta el **[Usuario]**.
    - No – La Documentación no está correcta o completa. Se devuelve la misma al **[Usuario],** explicándole las correcciones que debe llevar a cabo. Luego este debe volver a realizar la presentación de la documentación correcta y completa ante el **[Responsable del ALTA].**
7. El **[Responsable del ALTA]** firma el formulario.
    a. *Quedo pendiente de definir quién es el que firma en "Firma y Sello del propietario de los datos (Jefe de Repartición)". Hay que definir claramente que nivel jerárquico es el que debe firmar aquí.*
8. El **[Responsable del ALTA]**, en presencia del **[Usuario]**, da de alta el nuevo usuario en el Sistema SIIF y lo asocia, o crea, el perfil correspondiente.
9. El **[Usuario]** genera la contraseña correspondiente.
10. El **[Responsable del ALTA]**, procede a archivar la Solicitud "Alta de Usuario Sistema SIIF".

Protocolos

Figura 23 – Detalle de Actividades del Proceso: *Alta de Usuario Sistema SIIF.*



SAN JUAN

Gestión del Documento

A. Historial de Cambios

Fecha	Versión	Autor	Detalle
01Dic17	1.0	Horacio SANCHEZ	Creación.

B. Revisión

Revisión	Rol

C. Aprobación

Aprobación	Rol

Proceso: *Alta de Usuario Sistema SIIF* - V. *1.0* - SGP - Gobierno de San Juan Página 2 de 2

Figura 24 – Hoja de Gestión de Documentos – Detalle de Actividades: *Alta de Usuario Sistema SIIF.*

Gestión de Infraestructura TI

Esquema de Infraestructura TI asociada al Sistema SIGED

Se llevó a cabo el relevamiento de la Infraestructura de TI relacionada con el Sistema SIIF. Esto en función a lo mencionado, de tomar este sistema como la base del desarrollo futuro del Sistema Integrado a nivel Provincial.

La infraestructura relevada, corresponde al Sistema SIIF en su conjunto, el cual abarca claramente al SIGED. Es oportuno aclarar que el SIGED está en desarrollo, por lo cual es necesario incorporar nuevos componentes servidores e instancias virtuales producto de la expansión del mismo.

Desde esta consultoría se trabajó en el modelado de la infraestructura, con el fin de definir una base de documentación uniforme para referencia de todas las partes involucradas en el proyecto. Si bien existía información en formato de texto en planillas, se volcó la misma en diagramas de Microsoft Visio, a fin de definirlas como estándar.

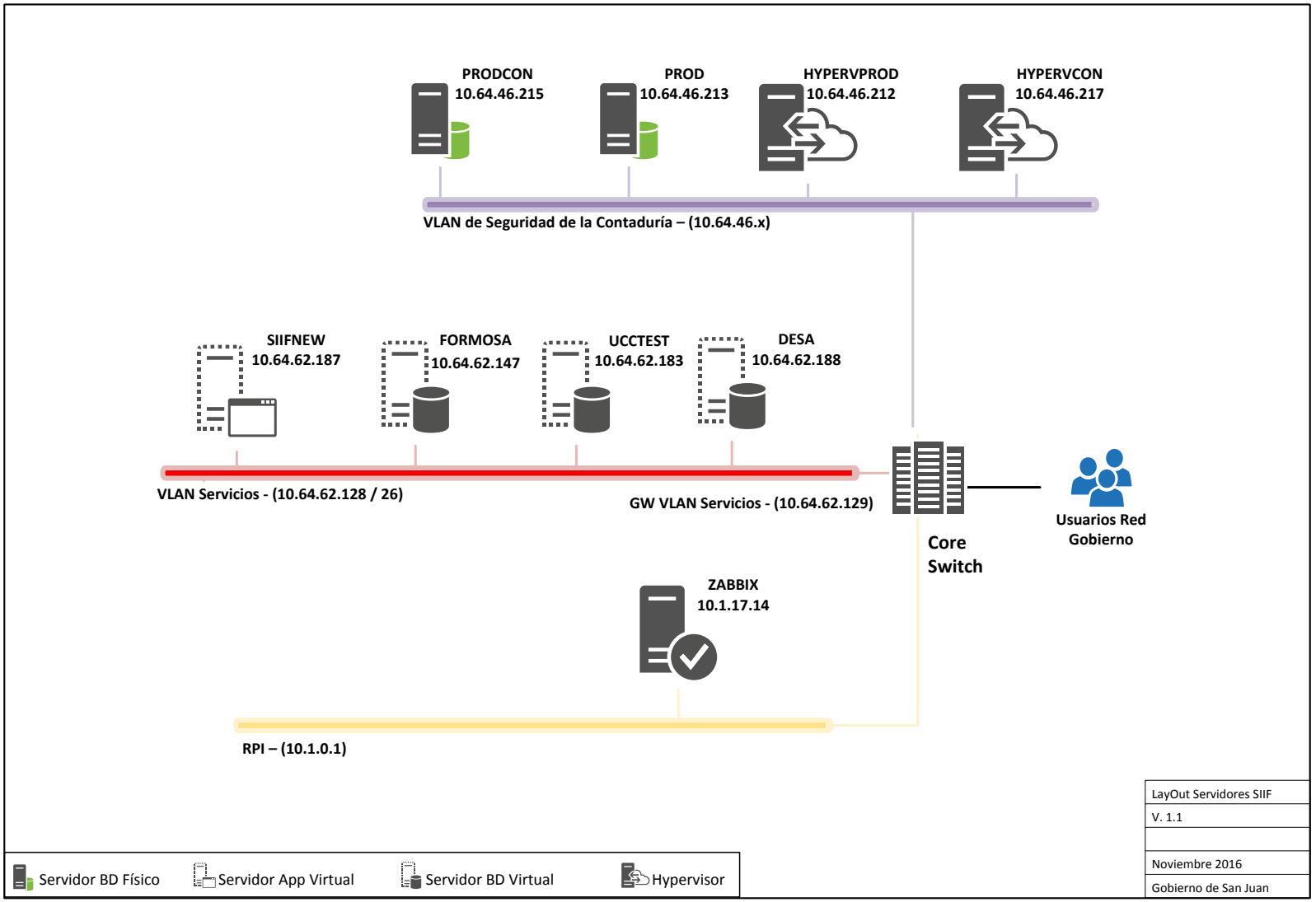


Figura 25 – Despliegue de la Infraestructura TI asociada al Sistema SIGED

En la Figura 25 se ha modelado el esquema de conectividad y despliegue de los componentes servidores e instancias virtuales. Las tres redes graficadas, corresponden a parte de la red física del Edificio del Centro Cívico. La red “Amarilla” corresponde a la Red MAN de Fibra Óptica actualmente bajo administración de la DPI. Sobre esta red se está implementando el Servidor con Zabbix.

La red “Roja” representa la DMZ actual de la red del Edificio del Centro Cívico (10.64.62.128/26). Sobre esta red están conectadas las instancias virtuales de los servidores de aplicación y Base de Datos de los Sistemas Integrados. Es también conocida como la VLAN de Servicio.

La red “Morada” representa la red de seguridad de la Contaduría sobre la cual están conectados los servidores físicos asociados a los Sistemas Integrados.

Las 3 redes están conectadas centralizadamente a través del switch central del edificio (conocido como CoreSwitch) el cual interconecta las redes mencionadas.

En el grafico (Figura 25) se visualiza el conjunto de “Usuarios Red Gobierno”, que representa el conjunto de VLANs que constituyen la totalidad de la conectividad del edificio. Las 3 redes mencionadas, están dentro del ámbito del Centro de Datos. Y los usuarios de la red de gobierno están fuera del ámbito del Centro de Datos.

Detalle de Virtualización

En la Figura 25 se presenta el Layout físico de los componentes que conforman y dan soporte al SIGED. Si bien se emplea tecnología de virtualización (Microsoft Hyperv) al momento de finalizar esta consultoría no se había alcanzado la consolidación a nivel de servidores en relación al Sistema.

La siguiente tabla detalla la relación entre componentes servidores y las instancias virtuales asociadas. La configuración actual está bajo la forma de el Hypervisor corriendo como servicio del NOS anfitrión. Se ha empleado como NOS Microsoft Windows Server 2008 R2, sobre el cual se levanta el servicio de Hyperv.

Servidor Físico		Instancia Virtual		
Nombre	**IP**	Nombre	IP	Rol /Función
HYPERVPROD	10.64.46.212	SIIFNEW	10.64.62.187	Servidor App
HYPERVCON	10.64.46.217	Antiguo TRADFIN	10.64.62.145	Servidor App
IBM 3650	10.64.62.186	FORMOSA	10.64.62.147	Base de Datos
IBM 3650	10.64.62.182	UCCTEST	10.64.62.183	Base de Datos
FLEX IBM		DESA	10.64.62.182	Base de Datos
PROD	10.64.46.213			Base de Datos
PRODCON	10.64.46.215			Base de Datos

Tabla 4 – Distribución de Instancias Virtualizadas

Una consideración importante es ir adaptando estándares al momento de la configuración y definición del esquema de infraestructura. Se trabajó en la definición de nombres adecuados para la denominación tanto de los Servidores Físicos, como de las Instancias Virtuales. Esto orientado a poder migrar fácilmente hacia un entorno de consolidación. La identificación precisa de cada uno de los componentes permite una interacción fluida entre las áreas involucradas. Es posible poder implementar soluciones de seguimiento y gestión de bitácoras (logs) de una manera natural y segura. Se trabajó en la implementación de estos tipos de soluciones en conjunto con el personal de la SGP. Mas adelante en el presente informe se presentará el modelo de monitoreo de infraestructura TI propuesto desde esta consultoría.

Monitoreo de Sistemas y Servicios

En base a requerimientos relevados a nivel de la Dirección Provincial de Informática (DPI) que depende de la Secretaría de la Gestión Pública (SGP), se inició con el estudio e implementación del monitoreo SNMP de los activos de red y diversos componentes. Estos componentes por monitorear son los pertenecientes, o que están involucrados de alguna manera, en la operación de los diferentes servicios y sistemas que gestiona la SGP.

Las posibilidades en cuanto a monitoreo que se presentan dentro de una organización a partir de la implementación del protocolo SNMP son muy amplias y

de una complejidad que puede volverse muy importante. Pudiéndose abarcar hasta la totalidad de los activos y servicios que implementen este protocolo. Una implementación global requiere de un proyecto de una envergadura considerable. Por lo cual, se propuso desde esta consultoría iniciar este proyecto focalizándose en un subconjunto bien definido de Sistemas y Servicios. Actualmente el Gobierno de San Juan está en etapa de desarrollo del Sistema SIIF como sistema central, y un subconjunto asociados de sistemas que operaran en forma integrada. Por lo descripto en el párrafo anterior, es que se tomó la decisión de llevar a cabo una implementación inicial acotada del monitoreo que tenga como alcance cubrir los sistemas y servicios asociados o involucrados en la implementación, operación y administración del sistema SIIF. Como así también algunos sistemas integrados relacionados a este.

Complementariamente se concretó el relevamiento de componentes de red asociados a la operación del SIIF, y servicios TI relacionados.

La Figura 25 ya presentada, representa el diagrama de red relevado, en el cual están graficados los componentes servidores asociados al SIIF como así también determinados activos de conectividad que participan de lo que se denominan conjuntos lógicos de monitoreo. Este último concepto de describirá con mayor precisión más adelante.

El alcance de esta consultoría tiene como base el estudio y soporte del SIGED. Pero en el ambiente que se ha definido desde la SGP, este sistema está fuertemente integrado con el sistema SIIF, que es el sistema madre o central al cual se irán integrando los restantes. Esta fuerte vinculación entre ambos sistemas, como así también entre los demás en desarrollo como el Sistema de Gestión de Obra Pública (SIGOP), Sistema del Instituto Provincial de la Vivienda (IPV), Sistema Integrado de Personas (SIP) y Sistema Integrado de Administración de Recursos Humanos (SIARH), conlleva que esta primera etapa de monitoreo involucre componentes comunes todos ellos.

Sistema de Gestión de Redes

Introducción

Toda organización, y en especial áreas de Gobierno, necesitan disponer de una red informática que facilite y acompañe el desarrollo de sus actividades. Dicha red estará formada principalmente por dispositivos de punto final (servidores, estaciones de trabajo, móviles, etc.), dispositivos complementarios, y otros activos de comunicaciones como routers, switches, impresoras, escáneres, etc.; todos interconectados de diversas maneras y niveles.

Independientemente del tamaño de la red, pero especialmente cuando la misma adquiere un volumen considerable, se hace necesaria la inversión fuerte y sostenida en recursos, procesos y personal para su administración. La labor de los administradores consiste en el diseño, despliegue, mantenimiento y monitoreo de todo el conjunto de Infraestructura TI. El mantenimiento involucra principalmente resolver los problemas de hardware y software que puedan presentarse en un tiempo aceptable. Complementariamente, mantener el monitoreo y posterior análisis de los datos recogidos ayuda a los administradores a optimizar el uso y gestión de los recursos que la componen. y prevenir futuros fallos o funcionamientos anómalos concurrentes.

Para realizar estas tareas, los responsables de la infraestructura de red cuentan con un conjunto de herramientas, y una de la más importantes son los Sistemas de Gestión de Redes (SGR) o NMS (en inglés *Network Mangement System*)

Descripción de un SGR

Un SGR es un conjunto de aplicaciones que tiene la capacidad de recolectar datos remotos y en tiempo real de los dispositivos y servicios que se deseen monitorizar. Estos datos serán enviados al servidor del SGR para ser analizados a través de un agente, empleando el protocolo SNMP (Simple Network Management Protocol), etc.

Es posible acceder al sistema en forma remota, mediante una interface web y facilita el análisis de componentes monitoreados que fallen o presenten un rendimiento distinto al esperado. También es posible definir notificaciones o alertas

(mediante email, SMS o diversos protocolos) en caso de que se produzca una situación anómala, la cual debe haber sido previamente definida por la gestión.

Un SGR permite:

- El descubrimiento de dispositivos y componentes de red, identificando qué dispositivos están presentes en la red, o son alcanzables mediante la misma.
- La monitorización de los dispositivos y componentes, analizando la red a nivel de dispositivo para comprobar la salud tanto del dispositivo de red como de la red por la cual es alcanzado.
- El análisis de la red, recopilando información como la utilización del ancho de banda, pérdida de paquetes, latencia, disponibilidad y el tiempo de actividad de los routers, switches y otros dispositivos que soporten y tengan activado el protocolo SNMP.
- Alertas inteligentes, mediante la configuración de escenarios de red en los que se lanzarán alertas mediante emails, sms, etc.

A pesar de que existen SGR propietarios, los sistemas Open Source son muy comunes y empleados actualmente. Así, el Sistema Zabbix es muy difundido. Una de sus características principales es ser un SGR completo y personalizable.

Objetivos y Justificación de un SGR

Todo sistema falla y las redes no son la excepción. Tomando lo anterior, lo que se busca es que esos fallos sean evitables y su resolución se logre en el menor tiempo posible.

Una manera de minimizar la ocurrencia de fallos es adelantándose a su ocurrencia. Para conseguirlo hay que utilizar una serie de herramientas que realicen un seguimiento continuo sobre la red en funcionamiento de manera que, al observar un descontrol, cambio brusco, o evolución no deseable de algún parámetro, se puedan tomar las medidas necesarias para evitar consecuencias mayores.

Para solucionar un problema de manera más rápida es conveniente tener un conocimiento temprano de la incidencia, y cierta certeza sobre la causa del mismo. Justamente el SGR se especializa en la manipulación de estos cometidos. Estos sistemas además de ser beneficiosos en la gestión de la red, para mejorar su eficacia, son muy buenos para que la red y los componentes complementarios tiendan a la eficiencia en su operación. Estas mejoras que se logran a partir del uso de estos Sistemas impactan también sensiblemente en el factor económico. Ciertas inversiones se ven reducidas al tener correctamente implementado un SGR. Estas inversiones pueden ser sistemas para reemplazar por daños sucesivos, tiempos de restauración de servicios, gastos en desplazamiento de personal, etc. El prevenir ayuda a no tener que reparar. Hay diferencias notables de costos, al lograr la resolución de incidentes en sus estados iniciales. Además, el contar con la mayor cantidad de información posible ayuda considerablemente a la hora de la resolución de los fallos *in-situ*. Y fundamentalmente, es posible incrementar notablemente los tiempos de disponibilidad de la infraestructura en su conjunto.

Otro beneficio es conocer las estadísticas y uso que los usuarios y otros sistemas hacen de la infraestructura y servicios ofrecidos, comprobando su utilidad. Definiendo métricas. A partir de esto es posible modificar estrategias en base a su utilidad y necesidad.

Por los factores enunciados, puede analizarse y medir la utilidad y el impacto de la implementación de un SGR dentro de una organización.

En el ámbito de la Administración Pública Provincial, desde la visión de esta consultoría, sería un sistema necesario y fundamental para implementar. Más adelante, se irán planteando premisas de diseño e implementación que fundamentarán lo aquí propuesto respecto a un SGR en el ámbito del Ejecutivo Provincial.

Sistema Zabbix

Fue creado por Alexei Vladishev, y actualmente es desarrollado y apoyado activamente por Zabbix SIA. Es una solución basada en código abierto de monitorización distribuida de clase empresarial. Supervisa numerosos parámetros de

una red y el estado de salud e integridad de los servidores y componentes de la infraestructura TI. Posee un mecanismo de notificación flexible que permite a los administradores configurar alertas basadas en correo electrónico para prácticamente cualquier evento. Esto contribuye a una reacción ágil ante los inconvenientes que se presenten en los componentes seguidos o monitorizados.

Ofrece excelentes funciones de generación de informes y visualización de datos basados en la información almacenada en la Base de Datos. Esto contribuye a la planificación de la capacidad y crecimiento de la infraestructura TI.

Zabbix soporta tanto sondeos como capturas. Todos los informes y estadísticas, así como los parámetros de configuración, se acceden a través de una única interface Web. Esta interface Front-End asegura que el estado de la red y la salud de los servidores se pueden evaluar desde cualquier sitio o ubicación. Configurado correctamente, como SGR, puede desempeñar un papel importante en el monitoreo de la infraestructura asociada. Es posible escalar desde pequeñas organizaciones con algunos componentes servidores hacia las grandes, con una multitud de servidores.

El licenciamiento de Zabbix es libre de costo, y está desarrollado y distribuido bajo la licencia GPL (en inglés, General Public License), Versión 2. Esto significa que su código fuente está libremente distribuido y disponible para el público en general. El apoyo comercial está disponible y proporcionado por Zabbix Company.

Vista General de Zabbix

Arquitectura

Zabbix se compone de varios componentes de software importantes, cuyas responsabilidades se describen a continuación:

- **Servidor:** El servidor Zabbix es el componente central al que los agentes informan la disponibilidad y la integridad de la información y las estadísticas. El servidor es el repositorio central en el que se almacenan todos los datos de configuración, estadísticos y operacionales.

- **Almacenamiento de base de datos:** Toda la información de configuración, así como los datos recogidos por Zabbix se almacenan en una base de datos. Nativamente se emplea MySQL como base de datos, pero por razones de escalamiento es posible emplear otras alternativas, como puede ser PostgreSQL.
- **Interfaz Web:** Para un fácil acceso a Zabbix desde cualquier lugar y desde cualquier plataforma, se proporciona la interfaz basada en web. La interfaz es parte del servidor de Zabbix, y nativamente (pero no necesariamente) se ejecuta en la misma instancia que la que ejecuta el servidor. La interfaz web de Zabbix debe ejecutarse en la misma máquina física si se utiliza SQLite.
- **Proxy (delegado):** El componente proxy de Zabbix puede recopilar datos de rendimiento y disponibilidad en lugar del servidor Zabbix. Un proxy es una parte opcional del despliegue de Zabbix; Sin embargo, puede ser muy beneficioso distribuir la carga de un solo servidor Zabbix. Esto en especial en Infraestructuras distribuidas como es la propia del Gobierno de la Provincia de San Juan. Este punto merece un análisis particular, sin duda alguna.
- **Agente:** Los agentes se implementan en objetivos de monitoreo para monitorear activamente los recursos y las aplicaciones locales y reportar los datos recopilados al servidor Zabbix. Es bueno aclarar que hay ciertas funcionalidades de monitoreo y control en las cuales no es necesario la implementación de agentes.
- **Flujo de datos:** Es importante tener bien claro el flujo de datos general dentro de Zabbix. Para crear un elemento que reúna datos e información, primero se debe crear un “host”. Complementariamente se debe crear un objeto para crear un disparador (*trigger* en inglés). Un disparador debe existir para crear una acción, este la determina. Por lo tanto, si se desea recibir una alerta de que la carga de la CPU es demasiado alta en el Servidor X, primero debe crear una entrada de host para el servidor X, seguida de un elemento para supervisar su CPU, luego un disparador que se activa si la carga de la CPU es demasiado alta, y envía mediante una “acción” un correo electrónico. Aunque esto puede suponer una elevada

complejidad, con el uso de plantillas que ya están definidas en el Sistema realmente no lo es. Sin embargo, debido a este diseño es posible crear configuraciones muy flexibles.

Operación del Sistema

Se describen a continuación una serie de pasos o configuraciones que definen la operatoria básica del proceso de monitoreo del Zabbix como SGR. Comprendiendo que estas configuraciones básicas permiten definir las bases correctas para el diseño adecuado del Sistema.

El “Servidor Zabbix”, es donde se configura y ejecuta la herramienta de Administración Web (Front-End). Mediante esta interface se deben registrar los equipos y dispositivos que van a ser monitoreados.

El “Agente Zabbix” debe estar instalado en el servidor o estación de trabajo que se desea monitorear y configurado para ser capaz de reportar al “Servidor Zabbix”.

El equipo “registrado” se convierte en un elemento a ser monitoreado y recibe el nombre de “Host”. Cada “Host” está compuesto a su vez por elementos llamados “ítems”, que básicamente son módulos que recogen y ordenan los datos del host.

Los “ítems” utilizan Claves (“keys” en inglés) que son parámetros de Zabbix. Las claves permiten indicar específicamente qué tipo de información se le desea solicitar al “Agente Zabbix”.

Los Triggers (disparadores) en Zabbix son módulos que se crean a uno o múltiples ítems para evaluar o comparar los valores recolectados por los ítems, con condiciones que previamente deben definirse. Por ejemplo, es posible crear un módulo “trigger” al item con Clave “Espacio Disco”, e indicar que si llega al 90% de espacio ocupado nos emita una alerta.

Funcionalidades

A continuación, se detallan un conjunto de funcionalidades bajo una visión global del SGR seleccionado.

- Alto rendimiento y alta capacidad (posibilidad de monitorizar cientos de miles de dispositivos).
- Auto descubrimiento de servidores y dispositivos de red.
- Monitorización distribuida y una administración web centralizada.
- Agentes nativos en múltiples plataformas.
- Posibilidad de monitorización sin agentes.
- Monitorización JMX. (Ver nota a continuación)
- Monitorización Web. Configuración de permisos por usuarios y grupos.
- Métricas SLA e ITIL.
- Sistema flexible de notificación de eventos (Email, SMS, XMPP, etc)

Nota: *JMX es Java Management Extensions. Del acrónimo Java Management eXtensions, JMX es la tecnología que define una arquitectura de gestión, la API (Application Programming Interface), los patrones de diseño, y los servicios para la monitorización/administración de aplicaciones basadas en Java.*

Nota: *IPMI es Intelligent Platform Management Interface. Nos permite gestionar Servidores y Blades con independencia de sistemas operativos y tipos de CPU. Como ejemplo se puede citar que los administradores pueden acceder a los sistemas y restablecerlos aún en el caso de que el sistema operativo no responda o el servidor se encuentre sin suministro eléctrico.*

Funcionalidades detalladas

A continuación, se presenta un listado bastante completo de las características de la versión 3.0 que se implementó en el ámbito de la Secretaría de la Gestión Pública. Si bien no se detallan ampliamente, las características enunciadas permiten obtener una visión global del sistema.

- Recolección de datos.
  - Comprobaciones de disponibilidad y rendimiento.
  - Soporte para SNMP (captura y sondeo), IPMI, JMX, monitoreo de VMware.
  - Cheques personalizados.
  - Recopilación de datos deseados a intervalos personalizados.
  - Realizado por servidor/proxy y por agentes.
- Definiciones de umbrales flexibles.
  - Puede definir umbrales de incidentes muy flexibles, llamados disparadores (triggers), referenciando valores desde la Base de Datos Backend.
- Alertas altamente configurables.
  - Las notificaciones de envío se pueden personalizar para la programación del escalado, el destinatario, o el tipo de medio.
  - Empleando variables macros, las notificaciones pueden ser más significativas y útiles.
  - Las acciones automáticas incluyen comandos remotos.
- Gráficos en tiempo real.
  - Los elementos supervisados se grafican de inmediato utilizando la funcionalidad gráfica que incorpora.
- Capacidades de monitoreo Web.
  - Zabbix puede seguir un camino de clicks simulados del ratón en un sitio web y comprobar la funcionalidad y el tiempo de respuesta.
- Amplias opciones de visualización.
  - Capacidad de crear gráficos personalizados que pueden combinar varios elementos en una sola vista.

    - Mapas de red.
    - Pantallas personalizadas y presentaciones de diapositivas para una vista general del Cuadro de Mandos.
    - Informes y Reportes.
    - Vista de alto nivel (Mandos Superiores) de los recursos supervisados.
- Almacenamiento de datos históricos.
    - Datos almacenados en una Base de Datos.
    - Historial configurable.
    - Procedimiento de limpieza incorporado.
- Fácil configuración.
    - Agregar dispositivos supervisados como hosts.
    - Los hosts son recogidos para el seguimiento, una vez que son incorporados a la Base de Datos.
    - Aplicar plantillas a dispositivos supervisados.
- Uso de Plantillas.
    - Agrupación de controles en plantillas.
    - Las plantillas pueden heredar otras plantillas.
- Detección de redes.
    - Descubrimiento automático de dispositivos de red.
    - Registro automático de agentes.
    - Descubrimiento de sistemas de archivos, interfaces de red y OID SNMP.
- Interfaz web rápida.
    - Front-End web en PHP.
    - Fácil accesibilidad desde cualquier lugar.
    - Puede hacer clic en su camino a través de registros de auditoría.
- API de Zabbix
    - La API de Zabbix proporciona una interfaz programable para manipulaciones masivas, integración de software de terceros y otros propósitos.
- Sistema de permisos.
    - Autenticación segura de usuarios.

    - Ciertos usuarios pueden limitarse a ciertas vistas.
    - Soporte a LDAP.
- Agente muy potente y fácilmente extensible.
    - Posibilidad de implementar el agente directamente en el dispositivo monitoreado.
    - Puede desplegarse tanto en Linux como en Windows.
- Demonios binarios.
    - Escrito en C, para optimizar rendimiento y uso de memoria.
    - Fácilmente portable.
- Soporte a entornos complejos.
    - Monitoreo remoto facilitado mediante el despliegue de un proxy de Zabbix.

Implementación de Zabbix en la SGP

Estado inicial del Servicio en la DPI

Al momento de iniciar esta consultoría en la DPI había una instalación de Zabbix (versión 2.2 LTS) ejecutándose sobre Ubuntu 12.04 LTS. Con esta implementación se monitoreaban dispositivos activos pertenecientes a la RPI (Red Provincial de Informática). A fin de complementar la infraestructura de monitoreo implementada hasta el momento, se trabajó para incorporar los dispositivos asociados al Sistema SIGED, e intentar realizar una actualización de procesos de gestión y formatos de visualización de los componentes.

Al comenzar a trabajar, se detectaron inconvenientes e inestabilidad en la interface Web del Sistema Zabbix. Complementariamente los datos almacenados asociados a los hosts configurados no estaban en condiciones de ser analizados. Se detectaron numerosos cortes en la continuidad del servicio de monitoreo.

Se intentó trabajar con los datos existentes, e intentar reestablecer el servicio. Para solucionar el problema se procedió a revisar cada uno de los componentes principales. Se revisó el Servidor Web Apache el cual se encontraba activo y funcionando correctamente (por lo cual era accesible la interfaz web), luego el servicio de Zabbix encargado del sondeo de los estados de los dispositivos a monitorear también se encontraba activo pero con inconvenientes al momento de almacenar datos. Se revisó el componente de almacenamiento (BD MySql) y este no estaba activo. Se analizaron varios factores y estados a fin de tomar una decisión.

Decisión de Actualización Integral

En conjunto con el personal técnico de la DPI, encargada de administrar la solución, se llegó a la decisión de realizar una actualización completa de la plataforma de monitoreo. Es decir, del SGR en forma integral.

Se procedió, desde esta consultoría a realizar una reinstalación y actualización a la última versión de MySql y de Zabbix. La última versión estable de Zabbix es la v 3.0. Dada esta nueva decisión, surgió el complemento de tener que actualizar la

versión de Ubuntu a la última versión estable también. Se procedió a instalar Ubuntu 16.04.1 LTS (Xenial Xerus) en una máquina virtual, administrada vía SSH.

Esta máquina virtual se conectó físicamente a la RPI, como originalmente estaba configurada. La IP asignada fue 10.1.17.14 que es la misma que tenía, de esta forma se evitaba impactar lo menos posible en las configuraciones existentes. Es fácil observar en la Figura N° 18, la ubicación lógica de la MV con Zabbix y el LayOut conformado.

Esta era la URL necesaria para acceder el Servicio Web de Zabbix del Ejecutivo Provincial: https://10.1.17.14/zabbix. Esta dirección inicialmente solo era accesible desde la intranet del Edificio del Centro Cívico.

Un punto sobre el cual se comenzó a trabar fue comenzar a modificar la configuración del Sistema Zabbix para llevarlo a un entorno de mayor conectividad. Es decir, conectarlo mediante interfaces virtuales a cada una de las VLANs a las cuales estuviesen conectados los Hosts monitoreados (“host” bajo la filosofía de Zabbix). Este nivel de configuración en lo referente a conectividad permite un monitoreo preciso y detallado de los entornos y los distintos componentes a monitorear. Más adelante en el presente informe se desarrollará en forma más detallada este concepto.

Proceso de Instalación de Zabbix

La versión que se instaló fue Zabbix es la 3.0.5 LTS, cumpliendo las siguientes etapas:

- Se realizó una actualización de los paquetes de instalación disponibles en los repositorios de Ubuntu.

- Se actualizaron las dependencias entre paquetes y sus versiones para iniciar con la instalación.

- Se descargó e instaló “Aptitude” para la instalación de paquetes y “Tasksel” para la instalación de paquetes y librerías relacionadas.

• Zabbix es administrado y operado mediante una interfaz web y complementariamente requiere de un gestor de Base de Datos. Por lo anterior se procedió a instalar un Servicio Web (Apache), un lenguaje de programación de servidor (PHP) y un Servidor de Base de Datos (MySql). Se decidió, en conjunto con personal de la DPI en implementar LAMP Server para satisfacer estos requerimientos.

Las versiones de los servicios desplegados fueron:

A. Apache V. 2.4.18
B. MySql V. 5.7.16
C. PHP V. 7

Complementariamente se instalaron los siguientes módulos adicionales para PHP:

A. **php-bcmath**: Para operaciones matemáticas de precisión arbitraria, la cual admite números de cualquier tamaño y precisión, representados como strings.
B. **php-mbstring**: Para utilizar esquemas de codificación multibytes de caracteres
C. **php-xml**: Para la manipulación de código XML

Una vez consolidada la infraestructura base para el Sistema se procedió a la descarga e instalación del paquete de Zabbix 3.0. Posteriormente se creó una Base de Datos vacía y se le aplicó el esquema descargado en conjunto con el paquete de Zabbix, estableciendo los permisos de acceso correspondientes.

Seguidamente se realizó la configuración de Zabbix para indicar la Base de Datos a utilizar, las credenciales para el acceso a la misma y otras configuraciones para el funcionamiento en Apache.

Una vez que la instalación y configuración básica estuvo completa y estable, se accedió a la interfaz web para cargar los dispositivos y configuraciones para

monitorear la accesibilidad al mismo, mediante el protocolo ICMP. Y se definieron las alertas correspondientes para el monitoreo de incidentes.

Los dispositivos cargados inicialmente fueron:

Item	Nombre
1	Core Switch
2	DB Prod
3	Desa
4	Desa FSA
5	HypevCon
6	HypervProd
7	Prod
8	Prodcon
9	Siifnew
10	TEST
11	Ucctest
12	Web Preprod
13	Zabbix server
14	Zeus

Tabla 5 – Lista de Dispositivos iniciales.

Diseño físico empleado para Zabbix

Como ya lo detallamos, en el ámbito de la SGP, esta consultoría llevó a cabo la implementación de un SGR orientado al soporte y monitoreo de los componentes asociados al proyecto del sistema SIGED. Se diseñó la implementación para que sea escalable con la vista puesta en la Infraestructura TI global del Ejecutivo Provincial. Lo anterior, siguiendo los lineamientos que definió la SGP del Ministerio de Hacienda y Finanzas.

En esta implementación se empleó tecnología de virtualización (VMware) que posee desplegada actualmente la DPI. Se creó una máquina virtual donde se instaló

el sistema Zabbix. Estas actividades se concretaron en conjunto con personal técnico de las diferentes áreas técnicas asociadas de la SGP.

Se crearon las reglas de acceso en el Core Switch de la red del Edificio, a fin de permitir el acceso al Front-End de Zabbix desde cualquiera de las VLANs que lo necesitaran.

Lo descripto corresponde al primer escenario montado para dar soporte a la solución de Zabbix.

Componentes de Zabbix

Grupos

Previamente a cualquier configuración se procedió a la definición de los grupos de usuarios. Zabbix responde al esquema de configuración de seguridad por grupos y herencia. Por lo cual, la primera medida que recomiendan las mejores prácticas es la definición de grupos de acceso y seguridad.

Los usuarios con los que se trabajó inicialmente fueron:

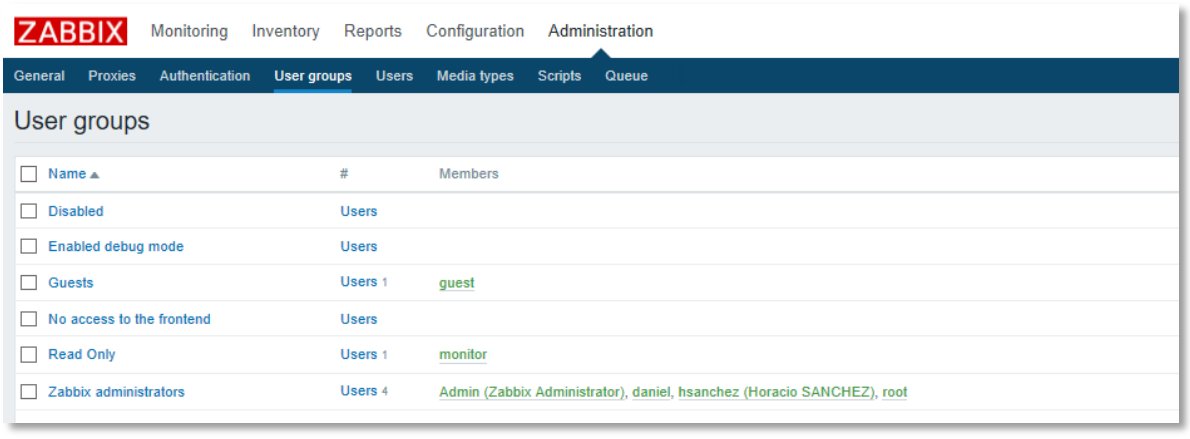


Figura 26 – Grupos definidos inicialmente en Zabbix

No se definieron grupos en esta etapa, ya que se comenzó a trabajar con los grupos predefinidos por el Sistema. El Grupo “Zabbix administrators” es el que posee los máximos privilegio a la hora de la configuración y administración del Sistema.

Un grupo importante en la implementación del Gobierno de San Juan, fue inicialmente un grupo con derechos de solo lectura (en inglés “Red Only”). A este grupo se le otorga permisos de acceso con privilegios de solo lectura, es decir que no puede realizar modificaciones, crear o borrar ningún objeto o propiedad de cualquier componente del Sistema. Solo posee privilegios de visualización.

Nota*: La interface presentada en la Figura 26, es la empleada para la consulta de Grupos del Sistema. La idea es ir presentado la información mediante las interfaces propias de Zabbix, a fin de que el usuario/lector se vaya familiarizando con el software.*

Usuarios

En esta primera etapa se procedió a la definición de usuarios genéricos. Si bien existen 2 niveles de acceso para la configuración del SGR, se priorizó la simplicidad a la hora de consultar la interface Web. En un principio se propone trabajar con consultas al SGR del tipo “*estado de salud*” de los Hosts. En la medida que el uso del Sistema se fuese intensificando, y los usuarios fueran familiarizándose con las interfaces, se avanzaría hacia esquemas de mayor complejidad y personalizados para la gestión de la infraestructura.

Así, se definieron los siguientes usuarios:

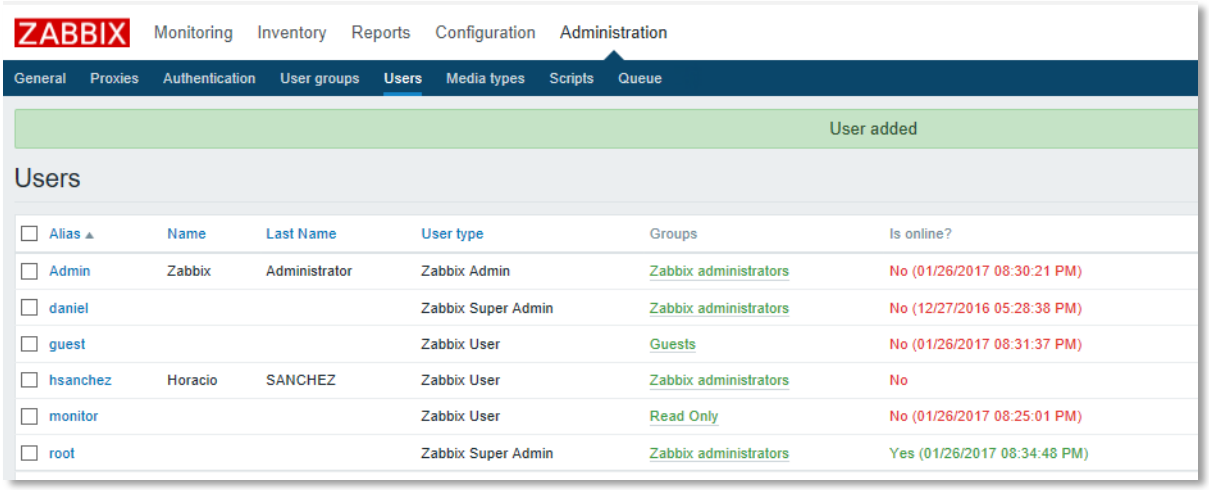


Figura 27 – Usuarios definidos inicialmente en Zabbix

El usuario sobre el cual se trabajó fuertemente en esta primera instancia es el usuario “monitor”. Inicialmente la filosofía definida, fue que cualquier persona que necesitara acceder al SGR, empleara este usuario (*monitor*) para realizar consultas del “estado de salud” de los distintos hosts definidos en el entorno Zabbix. En este primer período se dio especial enfoque a los hosts asociados al SIGED. De esta forma, fue posible mediante el uso de las credenciales de este usuario, tener acceso en modo “solo lectura” a todas las interfaces del Zabbix definidas.

En la Figura 27, se puede observar que el usuario “monitor” solo pertenece al grupo “Read Only”. Por lo cual hereda las propiedades y permisos de este grupo.

Grupos de Hosts

Bajo el mismo concepto planteado en la gestión y administración de Grupos de Usuarios, se debe enfocar en la creación de Grupos de Hosts. Es lo recomendable por las mejores prácticas también. Primero definir los grupos de Hosts, y posteriormente definir los Host y asociarlos a los grupos correspondientes.

Se configuraron tres (3) Grupos de Hosts, inicialmente. Estos son:

- PREPROD
- PROD

- Active Directory

En la siguiente figura, se pueden apreciar los tres (3) grupos mencionados, junto a otros grupos. Estos tres grupos están seleccionados y en amarillo.

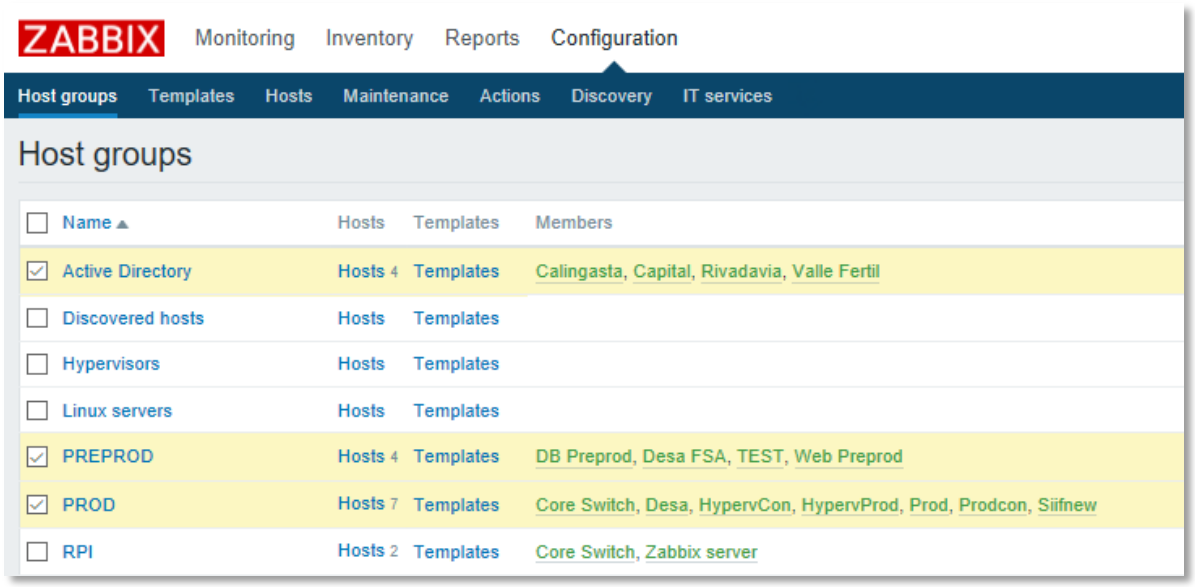


Figura 28 – Grupos de Hosts definidos inicialmente en Zabbix

Desde esta consultoría se propone adoptar esta filosofía para las definiciones de grupos. Es decir, la de poder operar con el concepto de Servicio. Un Servicio es una Unidad de Monitoreo, capaz de informar abstrayendo la complejidad del despliegue soportado. El Servicio permite focalizarse exclusivamente en el “estado de salud” del mismo. En este caso, podríamos entender que el Grupo de Hosts “PREPROD” define el Servicio de Preproducción (PREPROD). Este servicio engloba todos los hosts (host bajo el concepto de Zabbix) que permiten que sea posible operar contra la instancia de Preproducción del Sistema SIGED. Es decir, que todos los “hosts” que pertenecen al Grupo “PREPROD”, al estar activos, definen la operabilidad del “Servicio” PREPROD. El Servicio PREPROD, no existe esencialmente, sino que queda definido a partir de un requerimiento funcional y operativo de los objetivos organizacionales.

A nivel de la Secretaría de la Gestión Pública, se deberían ir definiendo los diferentes “Servicios”, a fin de ir determinando la configuración necesaria del Sistema.

La finalidad de este tipo de abstracción a la hora de definir Servicios para monitorear es que los distintos niveles de usuarios puedan tener una referencia básica y rápida del estado de la infraestructura TI que ellos emplean o les impacta.

Hosts

A continuación, se presenta el listado de Hosts, que se definieron en el Sistema.

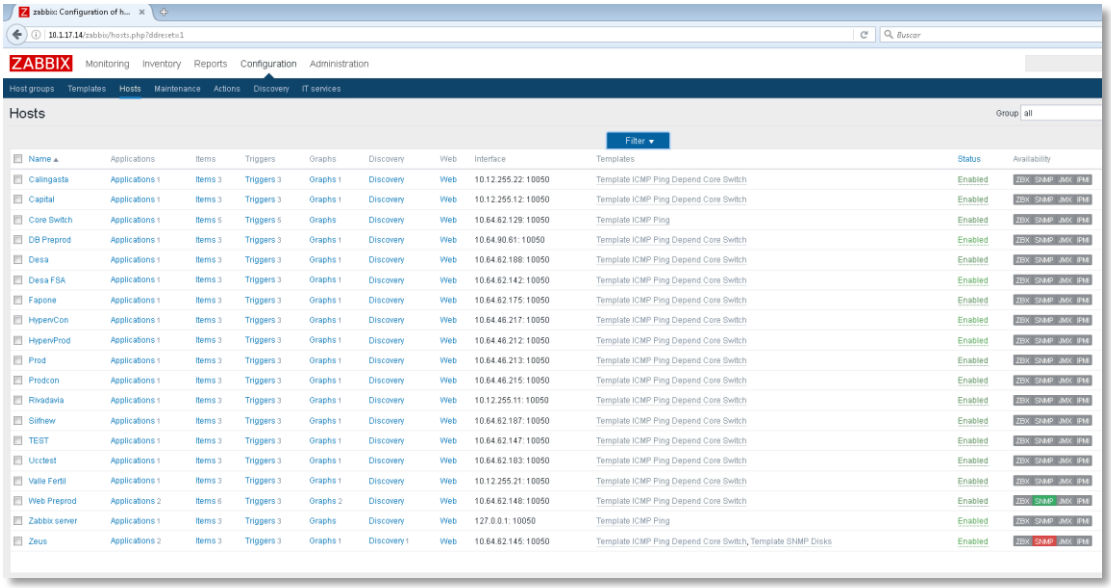


Figura 29 – Grupos de Hosts definidos inicialmente en Zabbix

Se puede observar que los hosts desplegados corresponden, en esta primera instancia, a componentes servidores (físicos y virtuales) e interfaces de red de activos de conectividad.

Así por ejemplo el Host de nombre “HypervProd” con IP 10.64.46.212, corresponde al Servidor Físico que opera como Hypervisor (ejecutando Microsoft HyperV como servicio). Sobre este Hypervisor se ejecuta la MV donde se corre la

instancia de producción del Servidor de aplicación del Sistema SIIF, que conjuntamente ejecuta la instancia del sistema SIGED.

Otro Host a tener en cuenta es el de nombre “Core Switch” con la IP 210.64.62.129. Este componente corresponde al Switch Central de la red del Edificio. Siendo este un activo de red aporta al Servicio “Prod” (ambiente de producción) la posibilidad de monitoreo de la conectividad asociada.

Mapas

Los mapas son representaciones gráficas activas de un conjunto de Hosts. Estas representaciones, contribuyen a un entendimiento y diagnóstico rápido el estado de los componentes que han sido configurados para su monitoreo. Se generan a partir de la inclusión en el mismo, de Hosts previamente definidos. Es posible establecer relaciones del tipo de conectividad entre los Hosts, a fin de poder representar de una forma más gráfica, y clara los diseños (*layouts*) típicos de la Infraestructura TI.

A continuación, presentaremos uno de los mapas generados oportunamente. Este es el mapa del Servicio de Directorio o *Active Directory*.

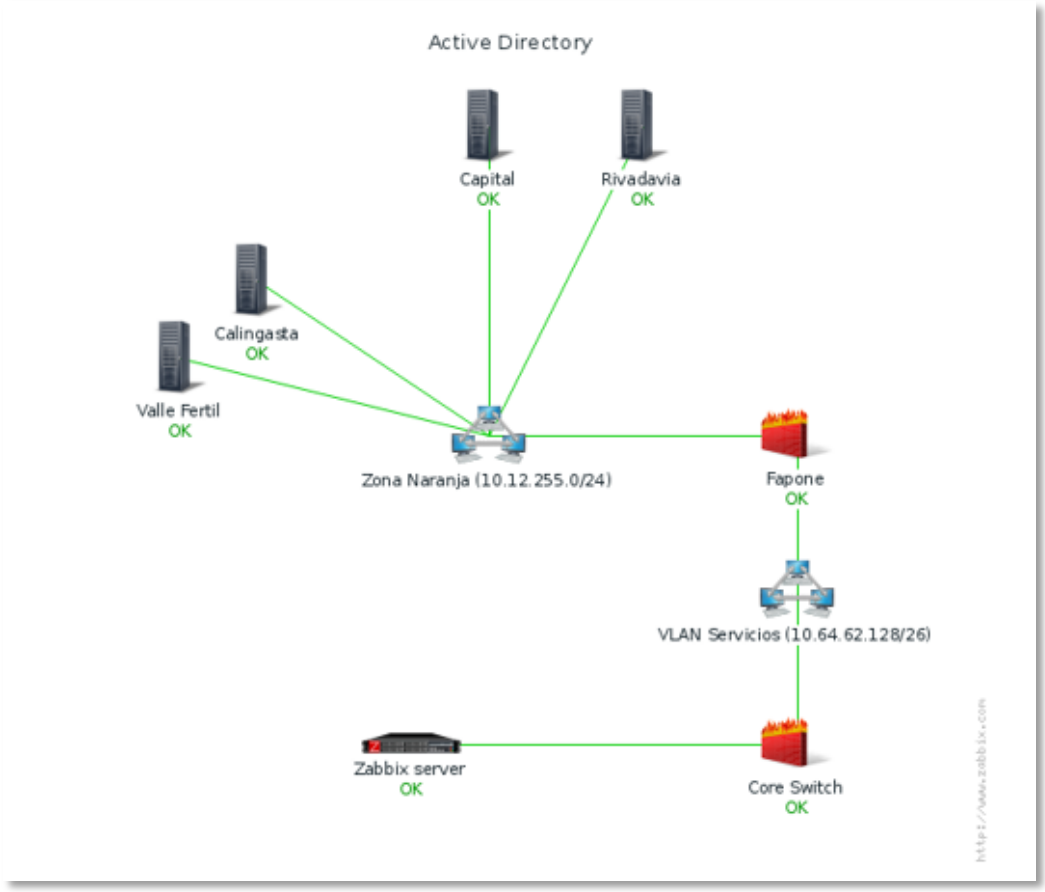


Figura 30 – Mapa Active Directory (Servicio de Directorio)

Este mapa intentaba representar los componentes involucrados que deben estar funcionando correctamente para que el Servicio de Directorio cumpla todas sus funcionalidades operativas. Y es posible ver en el, la relación a nivel de conectividad que posee con el Servidor Zabbix (host de nombre “Zabbix server”).

En este mapa se puede ver claramente, que para que el monitor Zabbix pueda monitorear los componentes (Hosts) propios del Servicio de Directorio (Rivadavia, Capital, Calingasta y Valle Fértil) deben estar operativo el “Core Switch”, la VLAN de Servicio, el Firewall “Fapone” y la VLAN definida como Zona Naranja. Esto es uno de los conceptos que se intenta implementar, el poder llevar a cabo el monitoreo en base a agrupaciones de Hosts, que representen funcionalidades operativas como serían los Servicios. Que definen estos “Servicios”. Entre el uso conjunto de Grupos de Hosts y Mapas es posible lograr ese nivel de abstracción.

Observemos ahora el mapa asociado al Ambiente de Preproducción del Sistema SIIF. Este mapa se definió en Zabbix con el nombre “Pre Producción”

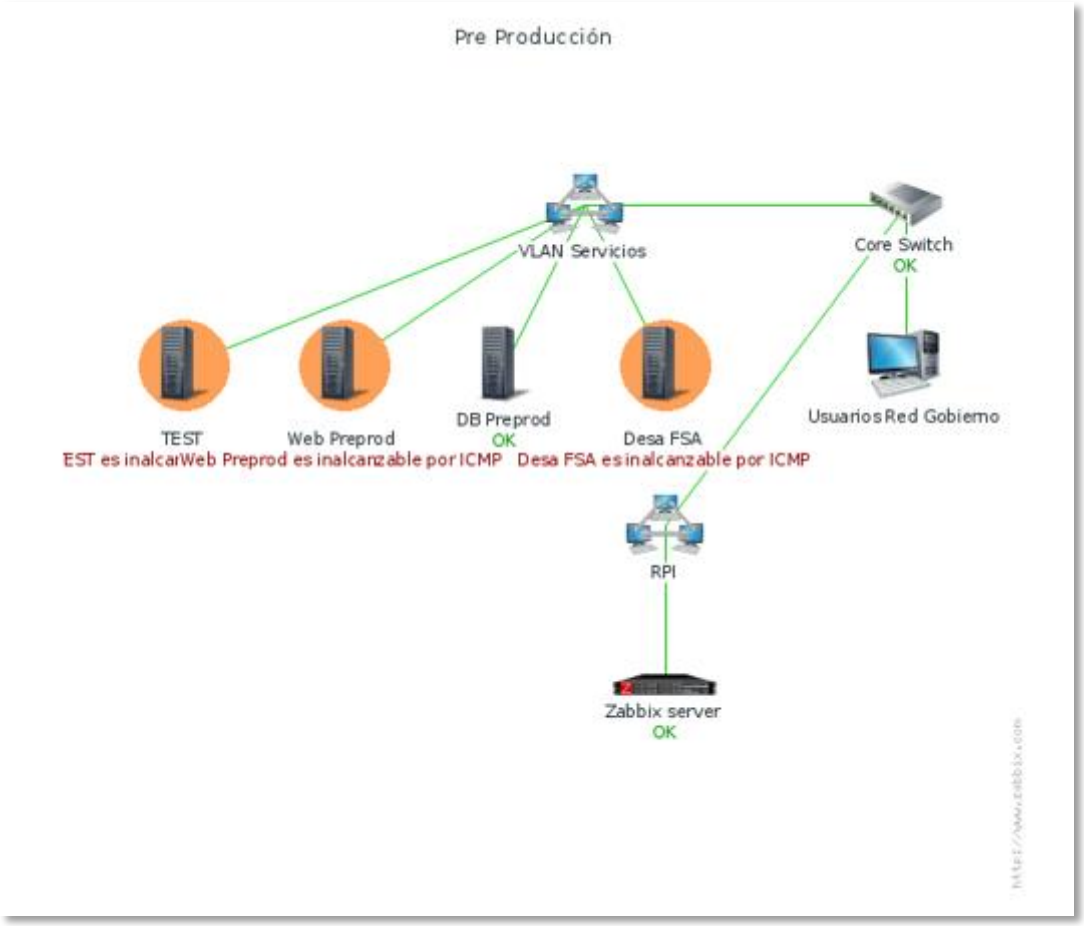


Figura 31 – Mapa Pre Producción (ambiente de Pre Producción del Sistema SIIF)

En este mapa se pueden observar los hosts que representan o conforman el ambiente de Preproducción del Sistema SIIF. Es claro aquí también, ver los componentes de conectividad involucrados y la ubicación de los Usuarios de la Red de Gobierno en cuanto al diseño de la infraestructura de conectividad asociada.

Los Componentes que poseen un circulo naranja detrás, representa que no están operativos. En este caso no responden al tráfico ICMP que emite el Servidor Zabbix. Es decir, ese host no está operativo, o activo.

La siguiente, Figura 32, presenta el 3° mapa generado. Este es el mapa del ambiente de Producción del Sistema SIIF.

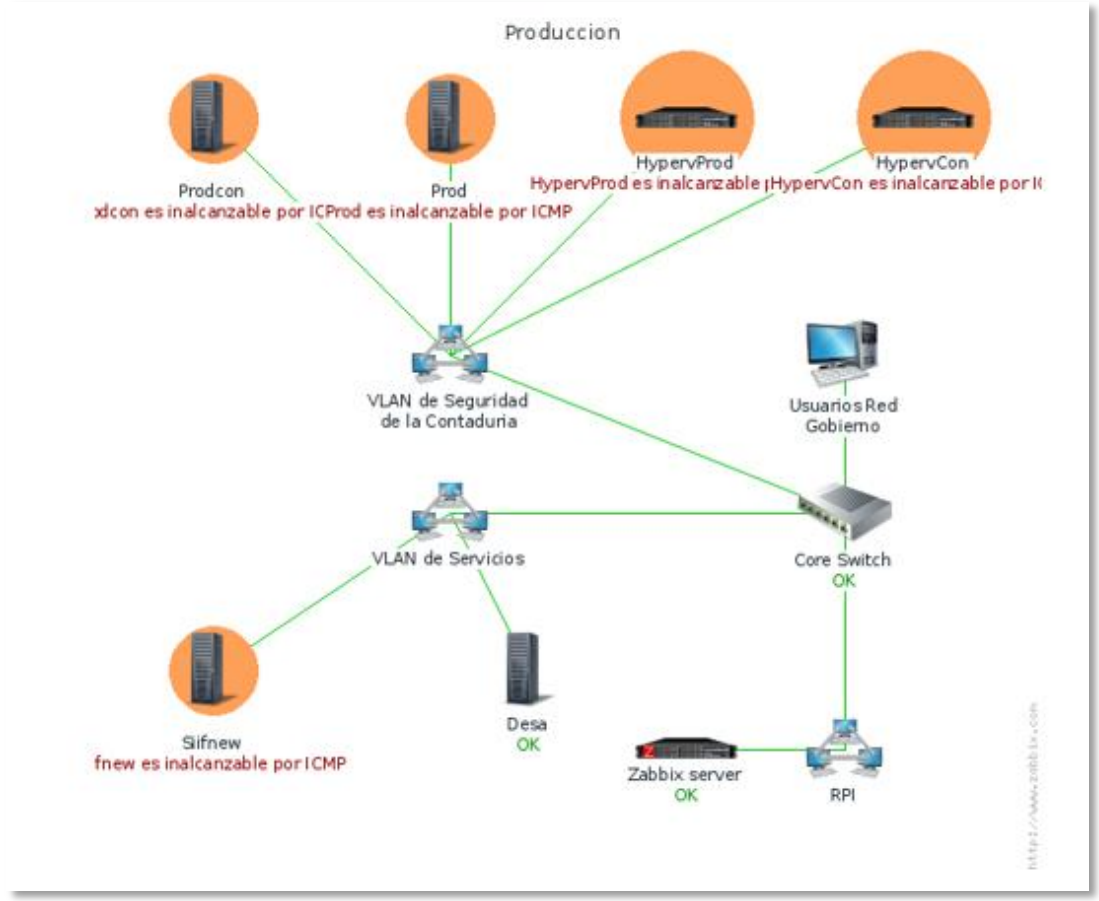


Figura 32 – Mapa Producción (ambiente de Producción del Sistema SIIF)

Como ya se presentó en el mapa anterior de “Pre Producción” es fácil observar que en este mapa hay cinco (5) Hosts que no están operativos. El monitoreo de estos componentes estaba momentáneamente desactivado de manera deliberada. Lo anterior fue debido a que, al tratarse del ambiente de producción, es conveniente llevar a cabo todas las pruebas en un laboratorio similar, antes de activar las reglas en el ambiente de producción propiamente dicho. El mapa presentado en la Figura 32, fue obtenido del ambiente de laboratorio montado oportunamente.

Como se puede observar, el poder contar con las representaciones gráficas de los diseños de infraestructura es altamente ventajoso, en contraposición a la posibilidad de poder observar los hosts monitoreados como simples tablas.

De todos modos, Zabbix también permite generar vistas diferentes a los mapas que tienden a ser de un nivel técnico de mayor especificidad. A continuación, veremos la vista del Dashboard principal de Zabbix, o vista basada en tablero.

Dashboard

El *Dashboard* o tablero, posibilita una visualización del estado de la infraestructura y componentes monitorizados desde un punto de vista especializado, técnicamente avanzado. Esta vista en formato de tablero puede ser parametrizada y completamente personalizada. A continuación, se presentará la vista definida actualmente en la instancia implementada en la SGP.

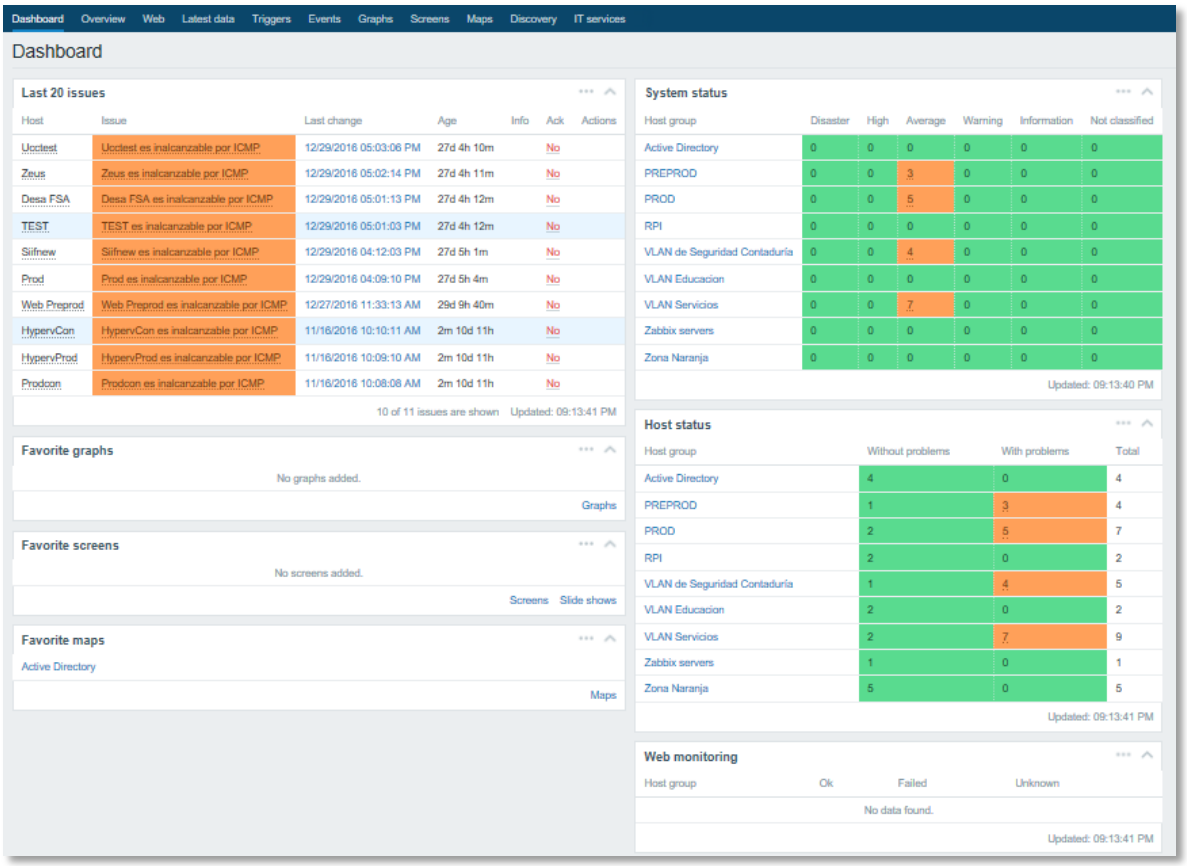


Figura 33 – Visualización del Dashboard principal de Zabbix

En el Dashboard, es posible apreciar un conjunto de elementos de visualización en forma ordenada y precisa. Esta vista fue modificada y se trabajó en ella con el fin de adaptarla a las necesidades de la SGP.

En el recuadro superior izquierdo (*Last 20 Issues*), se configuró para que se muestren los últimos 20 asuntos o inconvenientes que sucedieron entre los host definidos y monitoreados. Lo particular e importante de esta vista, es que muestra la fecha y hora del último cambio de estado de los hosts que tuvieron novedades.

El resto de los recuadros y áreas de esta interface permite ir agregando diversos tipos de representaciones que facilitan la interpretación y visualización de los eventos que impactan en la infraestructura de TI.

En los sucesivos informes se irán mostrando los diferentes tipos de estructuras que pueden ser montadas en el Dashboard para facilitar y colaborar con la administración y gestión de la infraestructura.

Así mismo es posible crear distintas vistas asociadas a ciertos usuarios. Es decir que se pueden definir vistas en relación con la estructura organizacional.

Es fácil visualizar en la Figura 33, en la esquina inferior izquierda, se pueden sumar los mapas ya definidos.

En la siguiente, Figura 34 a continuación, se muestra la capacidad para visualizar el estado de cada uno de los hosts a partir de la una de las estructuras de visualización como es el Estado de los Sistemas (en inglés, *System status*).

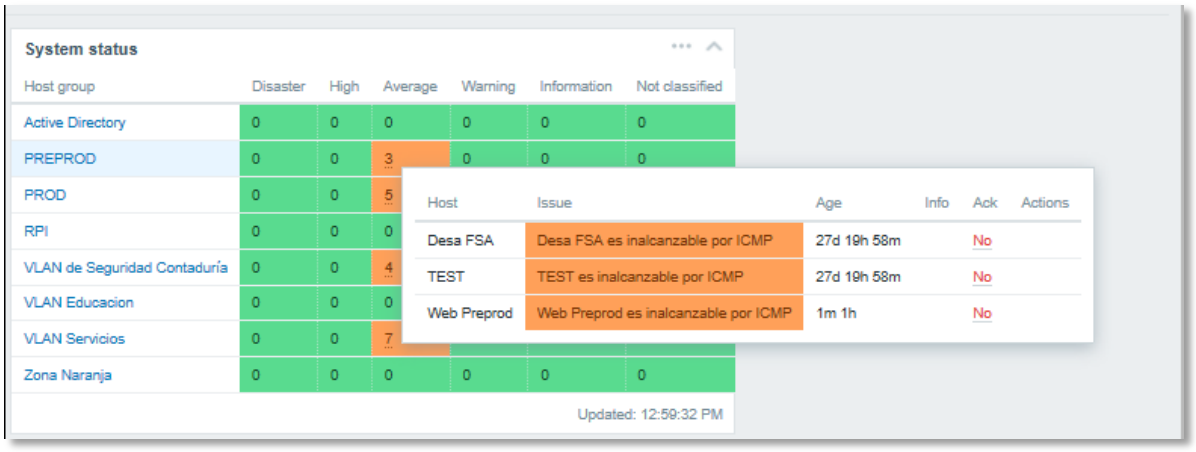


Figura 34 – Visualización del Dashboard principal de Zabbix

En la Figura 34 es posible visualizar el estado de los Grupos de Hosts. En las celdas de color naranja (resaltadas) es posible visualizar la cantidad de host que están con novedades dentro de cada uno de los Grupos de Host.

Así por ejemplo el Grupo de Host “Active Directory” no posee ningún host en estado de falla o en alerta. Toda la línea correspondiente a ese grupo está de color verde y con valores igual a 0 (Figura 35).

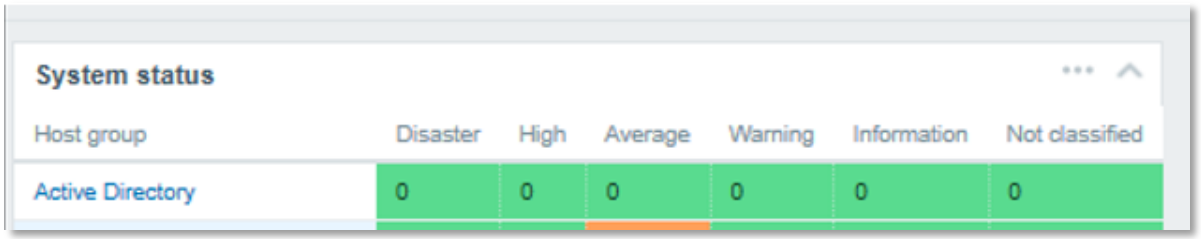


Figura 35 – Grupo de Hosts o “Servicio” completamente operativo, sin fallas o alarmas.

Esta estructura facilita enormemente la visualización del estado de los “Servicios” como hemos decidido definir en esta consultoría. Con una simple vista a esta estructura se sabe si hay algún incidente o falla.

En el caso del Grupo de Hosts “PREPROD” a simple vista se determina que hay 3 host que están en estado de falla. Y haciendo click sobre la celda naranja con el número 3, se despliega una ventana informando que Hosts son los que están con problemas y con el tiempo acumulado desde que se originó la falla (Figura 36).

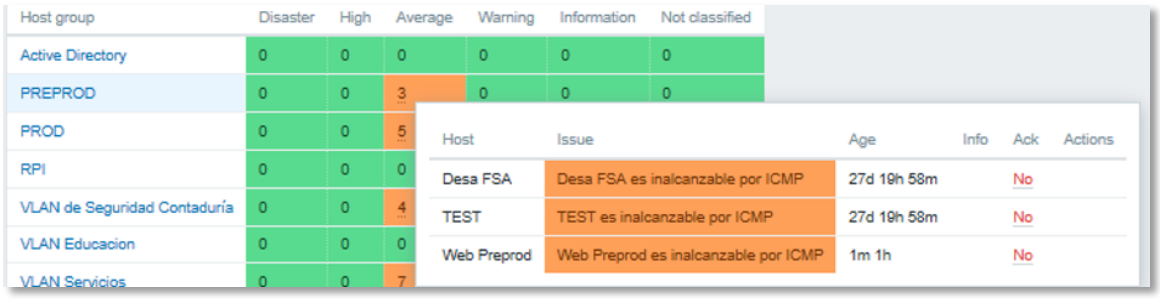


Figura 36 – Novedades de Hosts en estado de falla.

Toda la información presentada en este informe fue recolectada en el mismo instante de tiempo. Es decir que está relacionada. Por lo cual, si observamos la Figura 31, correspondiente al Mapa de “Pre producción” veremos una correlación total y completa con lo presentado en las Figuras 34 y 36. Es decir los 3 Host en estado de falla o novedad, son el “Desa FSA”, “TEST” y “Web Preprod”.

Estado actual de la Infraestructura

A modo de ejemplo se presentó el siguiente estado de la infraestructura al momento de tomar las imágenes correspondientes a las figuras de esta sección del informe. Cada uno de los Hosts está siendo monitoreado empleando el protocolo ICMP.

A continuación, se presenta el cuadro “System status” activo en ese momento.

System status

Host group	Disaster	High	Average	Warning	Information	Not classified
Active Directory	0	0	0	0	0	0
PREPROD	0	0	0	0	0	0
PROD	0	0	3	0	0	0
RPI	0	0	0	0	0	0
VLAN de Seguridad Contaduría	0	0	3	0	0	0
VLAN Educacion	0	0	0	0	0	0
VLAN Servicios	0	0	1	0	0	0
Zabbix servers	0	0	0	0	0	0
Zona Naranja	0	0	0	0	0	0

Updated: 10:15:43 AM

Figura 37 – System Status actual

En la Figura 37 puede observarse que dos (2) de los “Servicios” que se definieron para gestionar están 100% operativos. Estos son “Active Directory” y “PREPROD”.

Nota: *Se pueden observar diferencias entre las interfaces presentadas en las figuras anteriores y la Figura 37. Esto se debe a que las figuras anteriores se obtuvieron de un laboratorio montado para la probar la configuración inicial. Esta configuración luego fue migrada a la instancia de producción de Zabbix. De esta última se obtuvo la Figura 37.*

El “Servicio” de “PROD”, posee 3 componentes en estado de falla. Esto se debe que hasta el momento no se habían levantado el proceso de monitoreo en los servidores involucrados en el ambiente de producción.

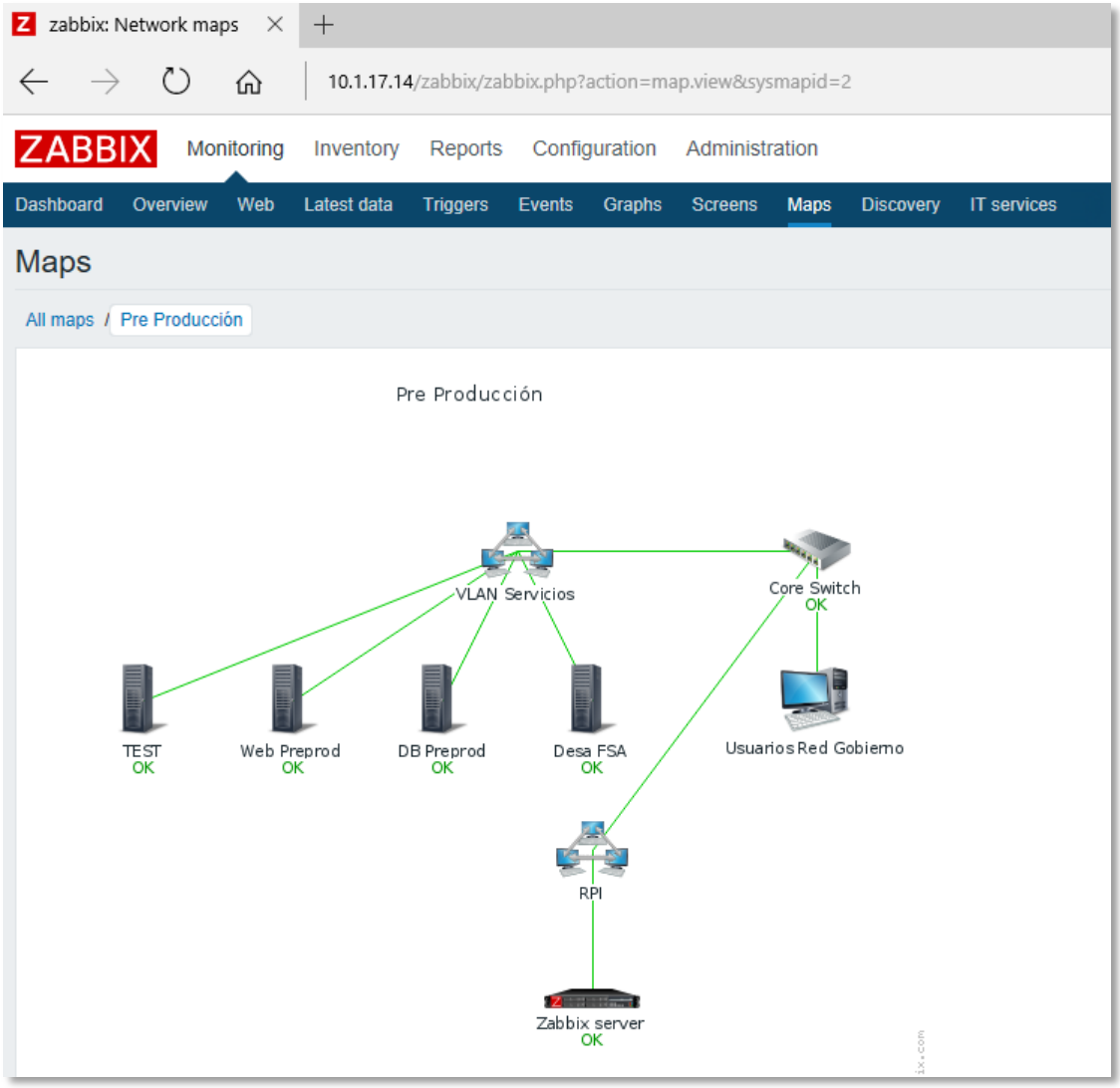


Figura 38 – Estado actual del Mapa de Pre Producción (PREPROD)

La Figura 38, muestra el estado del Sistema PREPROD en el momento de tomar las instantáneas

Normalización de Infraestructura

En conjunto con personal del área de Sistemas de la DPI, se acordó en comenzar a trabajar en la normalización de la infraestructura asociada tanto a los sistemas en producción como a los que están en desarrollo. La normalización propuesta involucra iniciar un proceso de evolución continuo que acompañe el ciclo de vida del desarrollo de la Infraestructura TI perteneciente de la SGP.

Naturalmente, toda área de TI tiende a crecer en forma relacionada o vinculada a los requerimientos y necesidades del día a día. Es común también observar un desarrollo asociado directamente con cambios en la realidad. Este crecimiento natural, es normal que se produzca cunado no hay un nivel de madurez adecuado dentro de la organización en cuanto a la gestión de recursos y procesos asociados.

Desde esta consultoría se propuso definir como objetivo organizacional avanzar en la normalización de la infraestructura hacia niveles superiores de madurez.

La infraestructura TI es un activo estratégico. Es una base fundamental sobre la cual los sistemas y servicios a proveerse pueden ofrecer lo que una organización moderna, como es la SGP, necesita para operar de manera efectiva y concretar sus objetivos organizacionales. Para muchas organizaciones, el crecimiento y el rápido desarrollo de nuevas tecnologías ha dado como resultado infraestructuras de centros de datos y de dispositivos de punto final demasiado complejas, inflexibles y difíciles de administrar. Seguramente también habrá una relación con costos asociados altos, que de alguna manera son fijos sin importar si se modifica los requisitos de las distintas áreas.

La mayoría de las organizaciones reconoce la importancia de una infraestructura de TI optimizada y controlada. Han intentado racionalizarla e incrementar su eficiencia operativa a través de iniciativas tales como la consolidación del centro de datos, la estandarización de escritorios, la implementación de mejores prácticas operativas de TI, etcétera. Tales iniciativas realizadas por los departamentos o áreas de TI de manera aislada no son suficientes por sí mismas para brindar las mejoras deseadas a largo plazo que demandan las organizaciones.

Las Organizaciones modernas deben definir una visión estratégica de mayor alcance para la madurez de su infraestructura. Y vincular esta visión a mejoras en capacidad, objetivos organizacionales y estrategia global.

Proceso propuesto para desarrollo de la Infraestructura

El proceso propuesto de optimización de la infraestructura ayuda a que las distintas áreas de la SGP logren grandes ahorros y simplificaciones a la hora de la

gestión de su infraestructura TI. Esto se logra al cambiar de un entorno no administrado y de crecimiento libre, a un entorno dinámico y controlado. El concepto es que la seguridad comienza a mejorar desplazándose desde un estado vulnerable en una infraestructura básica como se encuentra hoy, a una infraestructura más madura producto de ganar en dinamismo y proactividad. La administración de la infraestructura debería pasar de procesos manuales, aislados y reactivos a ciertos niveles de automatización y proactividad.

La propuesta es comenzar a incorporar tecnologías, procesos y procedimientos para ayudar a que la gestión de la Infraestructura avance hacia su optimización. Es importante que los procesos implementados, pasen de fragmentados o no existentes hacia procesos debidamente identificados, integrados, relacionados, optimizados y fundamentalmente repetibles.

Es crucial dotar a las áreas técnicas de procesos, metodologías y tecnologías para optimizar y mejorar la agilidad de la organización e incrementando su valor organizacional, conforme se incrementa el estado de optimización de gestión de la Infraestructura.

Al trabajar hacia la optimización y emplear un modelo como esquema, se puede comprender rápidamente el valor estratégico y los beneficios a nivel de objetivos organizacionales. Es fácil iniciar un cambio de un modelo de madurez “básico”, hacia un modelo más “dinámico”, donde el valor organizacional de la infraestructura TI se puede comprender con más claridad y comenzar a considerársela un activo estratégico de Gobierno. Y en especial como un habilitador de oportunidades organizacionales.

La idea subyacente del Modelo de Optimización de infraestructura propuesto es incorporar las buenas prácticas de la industria y las propias experiencias de Gobierno en estos últimos años.

El primer paso sobre el cual se inicia el trabajo es comenzar a identificar el nivel de madurez en el que se encuentra el Gobierno actualmente.

Nivel Actual Relevado

El Infraestructura TI de Gobierno actualmente se caracteriza por procesos manuales y localizados; un control central mínimo, pero en desarrollo; y políticas de TI también en proceso de desarrollo. Las normas relacionadas con la seguridad, respaldos, administración e implementación de imágenes, cumplimiento y otras prácticas comunes de TI también en proceso de desarrollo. Existe un conocimiento general básico relacionados con los detalles de la infraestructura con la que se cuenta actualmente o qué tácticas tendrán el mayor impacto para mejorar esto. Es básico el estado de salud general de las aplicaciones y los servicios, en parte a la falta de herramientas y recursos de monitoreo y auditoría. No existe un medio o vehículo para compartir el conocimiento acumulado en las distintas áreas que gestionan y administran Tecnologías de la Información. Suele suceder que los entornos de trabajo o producción sean difíciles de controlar, tienen costos muy altos de administración de escritorios y componentes servidores. Y por lo general son entornos reactivos a amenazas de seguridad, incidentes y errores funcionales. Los entornos de TI gestionados de esta forma suelen aportar poco en relación con los objetivos organizacionales. Gobierno obtiene beneficios básicos de su Infraestructura TI. Por lo general todas las revisiones, implementaciones de software y servicios conllevan un esfuerzo elevado y a costos considerables.

Las organizaciones se benefician mucho al cambiar de este tipo de infraestructura Básica a una infraestructura Estandarizada, ayudándoles a reducir en gran medida los costos en todas las dimensiones.

Objetivos Propuestos para la Optimización

Se propone iniciar un proceso de optimización de la infraestructura con el fin de convertirlo en un activo estratégico para Gobierno. Esta optimización se plantea definiendo como eje central el sistema SIGED.

Se debería iniciar el desarrollo de normas, políticas y controles orientado a definir una estrategia aplicable a mediano plazo.

Comenzar a disminuir los conflictos en seguridad, intentando desarrollar una postura de "defensa profunda": un enfoque en capas para la seguridad a nivel perímetro, servidor, escritorio y aplicación.

Iniciar la automatización de tareas manuales y que habitualmente consumen un tiempo considerable

Comenzar a considerar la adopción de “mejores prácticas” orientadas a la optimización de la infraestructura asociada al Sistema. Algunos de los estándares a considerar pueden ser la biblioteca de infraestructura de TI (ITIL), Marco de Referencia de Operación de Microsoft (MOF), el SysAdmin, Audit, Network, and Security Institute (SANS); Administración de Servicios de TI (ITSM), entre otros.

Iniciar el proceso de potenciar las áreas de TI para que aporten información estratégica.

En la siguiente sección se iniciará el planteo de una normalización en lo referente a infraestructura asociada al Sistema SIGED. Más adelante se irá avanzando en otros aspectos y líneas de acción.

Normalización de la Infraestructura asociada al SIGED

El proceso de normalización de la Infraestructura TI (ITI) puede tener un alcance lo suficientemente amplio como para abarcarla completamente. Si bien el alcance de la presente consultoría está vinculado directamente con el Sistema SIGED, se ha definido juntamente con el personal técnico de la SGP, de proponer directrices y definiciones que puedan ser aplicables a la totalidad de la ITI.

Proceso inicial de Normalización

Inicialmente, se ha tomado como base para el inicio del proceso la normalización de la infraestructura asociada al Sistema SIGED. Este proceso debe acompañar el ciclo de vida del desarrollo de la ITI, y esta etapa tiene por objetivo establecer un estándar de nombrado, documentación e identificación de componentes, servicios e instancias.

Modelado de Infraestructura

A continuación se presenta un diagrama del modelo de adminisgración básico de VMWare. Este representa un entorno de consolidación al cual se aspira dentro de la SGP. Si bien parte de la infraestructra TI ya está bajo este modelo, existen algunos componentes que están en vía de consolidarse bajo el mismo. En el caso de los componenetes asociadso al sistema SIGED, si bien se trabaja en un entorno virtualizado, se está pensando en migrar al siguente modelo.

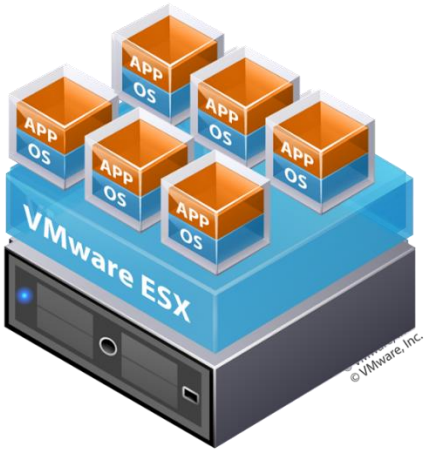


Figura 39 – Esquema de virtualización básico de VMware (Tipo 1).

En este modelo, sobre la infraestructura física TI, se implementa un hypervisor. Un hipervisor o como también se lo conoce monitor de máquina virtual es una plataforma que permite aplicar diversas técnicas de control de virtualización para utilizar, al mismo tiempo, diferentes instancias de sistemas operativos sobre una misma infraestructura física. El modelo al cual se apunta actualmente en el ámbito de gobierno es el conocido como Hypervisor de Tipo 1 (Figura 39).

Respecto al Sistema Integrado SIIF, actualmente corre sobre un entorno virtualizado empleado Microsoft Hyperv en modo no nativo. Es decir, virtualización

del Tipo 2. Con respecto a los motores de Base de Datos, no están virtualizados. Directamente se ha implementado la instancia del NOS sobre el hardware servidor.

Esta realidad de implementación conlleva a un escenario bastante heterogéneo. Se encuentran numerosos tipos de configuraciones, en escenarios muy diversos. Una buena práctica aconsejable en estos casos es comenzar a trabajar en la documentación e identificación de todos los componentes. Este trabajo contribuirá fuertemente en un futuro en darle continuidad a la transición del Tipo 2 hacia el Tipo 1.

La SGP ha iniciado un fuerte proceso de actualización de su Infraestructura de cómputo. Se prevé incorporar actualizaciones diversas al Sistema Flex de IBM, lo cual le permitirá absorber gran parte de los distintos sistemas y máquinas virtuales que actualmente posee distribuida en diversas infraestructuras. Lo anterior sumado a la infraestructura de virtualización, gestión de disponibilidad y contingencia implementada en el Sistema IBM mencionado, permitirá alcanzar un proceso de consolidación considerable.

Una vez que estén desplegadas las nuevas actualizaciones, será necesario llevar a cabo un proceso de identificación, documentación y reordenamiento de cada una de las MVs que se vayan incorporando al nuevo sistema. Este proceso de ordenamiento, sería aconsejable iniciarlo inmediatamente, intentando tenerlo lo más avanzado posible al momento de tener que llevar a cabo la actualización del sistema como se mencionó.

Complejidad a monitorear

Ya sea en un entorno de virtualización Tipo 1 o Tipo 2, la complejidad que se presenta es considerable. En especial cuando comienza a incrementarse gradualmente el número de máquinas virtuales a partir de requerimientos aislados que no han sido producto de un diseño y planificación previa. Esto es común en ambientes donde se inicia un fuerte proceso de crecimiento y actualización como el que se está llevando a cabo en el ámbito de la SGP. La implementación de numerosos sistemas, con sus respectivos entornos de capacitación, desarrollo y pre Producción; demandan una dinámica considerable a la hora de acompañar los

requerimientos desde las áreas de Infraestructura. Es bueno recordar que actualmente la Secretaría de la Gestión Pública lleva adelante un ambicioso proyecto de actualización y desarrollo de nuevos sistemas, los cuales operan de forma integrada, lo que demandará a futuro un incremento considerable a nivel de componentes de cómputo.

Ahora bien, este proceso iniciado por la SGP, complementado con una fuerte decisión de avanzar en la consolidación del Centro de Datos, determina la necesidad imperiosa de iniciar un proceso de normalización y reordenamiento de su infraestructura TI. Conjuntamente, surge naturalmente la necesidad de iniciar también un proceso de seguimiento y monitoreo de los componentes que conforman esta infraestructura.

Consideramos bueno entender la complejidad asociada a la tecnología que se opera actualmente, y que se verá incrementada sustancialmente en un futuro. La siguiente figura, presenta de forma simplificada el conjunto de componentes tecnológicos que se deben identificar con claridad.

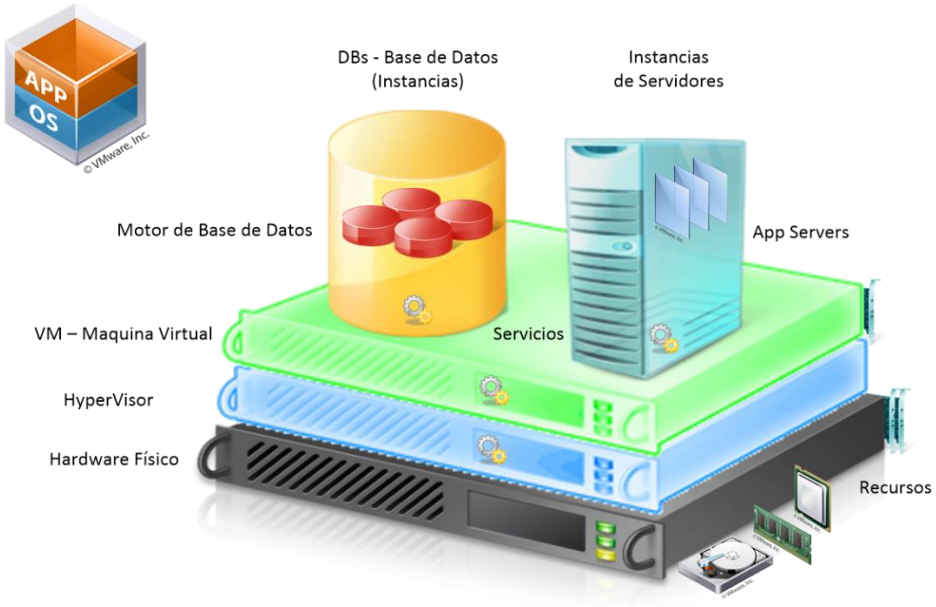


Figura 40 – Componentes factibles de monitorear empleando SNMP.

Nota: *Es bueno aclarar que lo presentado a continuación debe ser interpretado desde un punto de vista de monitoreo y gestión tecnológica. Es decir que los componentes identificados y relevantes, son aquellos que pueden ser documentados y/o monitoreados por softwares del tipo SGR.*

A modo de ejemplo se presentará el Sistema FLEX, y su arquitectura de hardware asociada. Esta arquitectura es una de las empleadas dentro del ámbito de Gobierno. También es posible encontrar otras alternativas, pero se empleará esta en este informe.

En la Figura 40 se presenta un primer nivel (Hardware Físico) el cual está constituido por el hardware propiamente dicho. Este conjunto está conformado tanto por el Sistema Flex propiamente dicho (o el Sistema Blade de la Contaduría o similar), como así también por Servidores físicos individuales, componentes de storage, etc. Sobre la derecha de este componente de color negro, se puede observar un conjunto de recursos sensibles a monitorear, como son los microprocesadores, memoria, almacenamiento o NICs por nombrar los principales.

El segundo conjunto o nivel (color azul) está representado por el software de virtualización o hipervisor. Este componente de software es central en el esquema de infraestructura que se ha elegido. Actualmente la SGP, ha adoptado el modelo de virtualización Tipo 1, empleando los productos VMware ESXi e HyperV de Microsoft. Ambos productos responden perfectamente a los requerimientos de una organización como es el Poder Ejecutivo Provincial. Desde esta consultoría se aconseja ir hacia la unificación en uno de ellos. Por la madurez de la implementación realizada, el nivel de licenciamiento y la capacidad de los RRHHs afectados a esta tecnología, se considera que se debe avanzar hacia la unificación en la plataforma de VMware.

El tercer conjunto, contando desde abajo hacia arriba en la Figura 40, es el correspondiente a las Máquinas Virtuales (MV). Representado en color verde. Cada una de las MV es un contenedor en sí mismo. Si bien comparten los recursos del hardware físico que les aprovisiona el hypervisor, posee recursos propios y posee el

nivel de aislamiento suficiente para operar independientemente de las restantes. De esta forma se constituye en una unidad perfectamente identificable e ideal a ser monitoreada. Cada MV posee sus propios recursos y configuraciones. Sobre este conjunto de recursos aparecen las instancias de los NOS (del inglés Network Operating System). Cada una de las MV posee su propio Sistema Operativo de Red.

Por último, es fácil identificar los dos últimos conjuntos de recursos, como serían los Servicios o Componentes Servidores y por último las instancias de estos Servicios. Así, el motor de Base de Datos Oracle, empleado para gestionar las Bases de Datos del Sistema SIGED, sería un ejemplo de servicio. Y las Bases de Datos de Desarrollo, Prueba y Producción definen el último conjunto, es decir las instancias. En este caso tres instancias.

A modo de simplificación, podríamos presentar los conjuntos mencionados como capas y agruparlas en un modelo integral. Así se puede presentar la siguiente tabla.

N°	Capa	Componentes
7	**Instancias**	Base de Datos.
6	**Servicios**	Aplicaciones, Motor de Base de Datos, Componentes Servidores (Oracle, IIS)
5	**NOS**	Instancia de NOS, Servicios de SO
4	**MV**	Memoria, Disco, NICs Virtuales,
3	**Hypervisor**	Software, Servicios.
2	**Hardware/Capa Física**	NICs Físicas, Memoria, Discos.
1	**Conectividad**	Activos, Gateways, Firewalls.

Tabla 6 – Modelo de Capas de Monitoreo.

En base a la Tabla 6, podemos incorporar el concepto de capas. Así, queda bastante gráfico el alcance de la agrupación de componentes, y el conjunto de recursos que determina cada una de las capas definidas.

Una capa sobre la cual no se habló hasta el momento, es la Capa 1. Esta está determinada por todo lo relacionado con la conectividad física de los componentes computacionales. Esta capa involucraría las 4 primeras capas del modelo ISO-OSI de conectividad.

Todo el desarrollo de este modelo se trabajó en conjunto con el personal técnico de la SGP, a fin de afinar conceptos y aspectos que permitan obtener un modelo de monitoreo que se ajuste a las necesidades del Gobierno Provincial.

La idea central es independizarse de la herramienta de software empleada. Ajustar el modelo necesario que cumpla con los requisitos de Gobierno, y luego adoptar y adaptar la herramienta.

Desde esta consultoría, en base a la experiencia de los consultores, se recomienda el producto Zabbix el cual se adapta inicialmente, permitiendo avanzar en la definición del modelo.

Proceso de Identificación de Componentes

Actualmente para llevar a cabo la Gestión de la Infraestructura el personal técnico emplea planillas con la información de componentes computacionales. Estas planillas se van generando en función de los requerimientos y necesidades que surgen de la gestión misma. Así es normal encontrar planillas generadas por el personal del área de Redes y Conectividad, de Servidores, y del área de Base de datos y Aplicaciones. Estas planillas, o documentos similares, contribuyen considerablemente a la identificación y documentación de cada uno de los componentes computacionales.

A continuación, se presenta la planilla relevada que se emplea en el Área de Base de Datos para documentar los servidores e instancias de Bases de Datos que se administran actualmente para el sistema SIIF.

Servidor Físico		Instancia Virtual			
Nombre	IP	Nombre	Nombre Instancia NOS	IP	Rol /Función
HYPERVPROD	10.64.46.212	SIIFNEW	SIIF-PROD	10.64.62.187	Servidor App
HYPERVCON	10.64.46.217	Antiguo TRADFIN		10.64.62.145	Servidor App
IBM 3650	10.64.62.186	FORMOSA	SERVER10	10.64.62.147	Base de Datos
IBM 3650	10.64.62.182	UCCTEST		10.64.62.183	Base de Datos
FLEX IBM		DESA		10.64.62.182	Base de Datos
PROD	10.64.46.213				Base de Datos
PRODCON	10.64.46.215				Base de Datos
HyperV	10.64.62.135	PREPROD	SIIFprePROD	10.64.62.148	Servidor App
PREPROD	10.64.90.61			(VLAN Educación)	Base de Datos

Tabla 7 – Listado de recursos computacionales actuales asociados al SIIF.

.

Esta tabla representa los “Servidores Físicos” y las “Instancias Virtuales” asociadas. En la primera columna se han definido nombres para los servidores que se acordaron en conjunto con el personal de la SGP, y la segunda columna presenta las direcciones IPs asociadas a esos servidores. En conjunto con personal técnico de Base de Datos, se trabajó en definir un conjunto de nombres para cada uno de los recursos que permita iniciar un proceso de identificación y de identidad para cada uno. Se propone, definir una nomenclatura o acuerdo previo, para respetar los nombres acordados en la medida que se vaya relevando toda la infraestructura.

En la 3° Columna figuran los nombres con los que se los conoce normalmente a estos “Servidores”. Es bueno aclarar que estos nombres suelen ser empleados por las áreas técnicas de la SGP y son de uso corriente. Luego, la 4° Columna [Nombre Instancia NOS] muestra los nombres de la instancia de los Sistemas Operativos (Máquinas Virtuales) sobre la cual se ejecutan los componentes servidores. Estos nombres son los empleados normalmente en las implementaciones de sistemas operativos Windows. Es el conocido como nombre NetBIOS. Como proceso complementario, y a nivel de infraestructura se debería iniciar la estandarización del uso del sistema DNS como nomenclatura jerárquica para redes IP. Y se debería establecer una correlación correspondencia entre los dos espacios de nombres.

La siguiente columna, la 5°, muestra la dirección IP (generalmente son IPs virtuales). Y finalmente la 6° Columna, presenta generalmente el rol o función que cumple la máquina virtual (3°Columna).

Ahora bien, analicemos que información está representada en la Tabla 7, tomando como base el Modelo de Capas de Monitoreo definido en la Tabla 6.

Se extrajeron algunos ejemplos, y se mapearon según el modelo planteado

Nombre	Función	Detalle	Capa Según Modelo
HYPERVPROD	Hypervisor	HyperV (Tipo 2) empleado para virtualizar el ambiente de producción de SIIF	3
PROD	Instancia de Base de Datos	Base de Datos de Producción del Sistema SIIF	7
SIIFNEW	Servidor de Aplicación	Servidor de Aplicación del Sistema SIIF	6

Tabla 8 – Mapeo de Componentes según Modelo de Capas de Monitoreo.

Es claro ver en la Tabla 8 como se mezclan componentes de distintas capas. Y, puntualmente hay ambigüedad a la hora de nombrar e identificar cada uno de los componentes servidores.

1. El componente de nombre “HYPERVPROD” es un servidor físico ejecutando un NOS Windows Server sobre el cual corre el Servicio de hypervisor empleando HyperV de Microsoft (Tipo 2).
2. El componente de nombre PROD, es un servidor físico ejecutando un NOS Windows Server sobre el cual correo el Motor de Base de Datos Oracle, sobre el cual se ejecuta la instancia (o Base de Dato) de Producción del Sistema SIIF.
3. El componente de nombre SIIFNEW es una Máquina Virtual con NOS Windows Server ejecutando el componente Servidor IIS (*Internet Information Server*) que opera como Servidor de Aplicaciones para el Sistema SIIF.

La planilla presentada en la Tabla 7, es muy útil y completa para el área técnica que la creó, y por lo general “solamente” para el técnico que administra dichos componentes. Dificulta sensiblemente la intercomunicación entre las distintas áreas técnicas y de toma de decisión.

Bajo otro punto de vista, presenta los inconvenientes de ser muy ambigua para el resto del personal, no es buena fuente de documentación y es muy compleja de mantener actualizada ya que no está basada en un modelo. No hay definidos criterios para su llenado y correspondencia.

Por lo planteado, se propone avanzar en la especialización del modelo enunciado, potenciándolo fundamentalmente como una herramienta de documentación. Esto permitirá y agilizará la interacción entre las diferentes áreas.

Al completar esta fase de relevamiento, identificación y documentación, será más sencillo poder emplear una herramienta de monitoreo (como puede ser Zabbix) para gestionar la Infraestructura

Agrupamiento y Simplificación

Como una etapa subsiguiente a la identificación, se propone comenzar a trabajar en la definición de conjuntos de componentes orientados a ambientes específicos. Es decir, crear una subclasificación o agrupamiento de segundo orden, que permita generar niveles adicionales de abstracción para la comprensión, entendimiento y gestión de la infraestructura.

De esta forma, se propone trabajar sobre el concepto de “Servicio” o “Ámbito”. Es decir, agrupar los componentes en relación con su función dentro del entorno de Infraestructura.

Así en base a lo relevado oportunamente se detectaron, entre otros, dos ambientes bien definidos. Uno es el ambiente de “Preproducción” y otro el ambiente de “Producción”. Estos dos ambientes se refieren a la implementación del Sistema SIGED, es decir la infraestructura desplegada para darle soporte al Sistema SIGED. El ambiente de Preproducción engloba todo lo necesario para poder desarrollar, probar y ejecutar el SIGED en un ambiente de prueba lo más similar posible al

entorno de producción. En este ambiente, trabajan conjuntamente los equipos de San Juan y Formosa para poner a punto las distintas versiones del SIGED antes de pasarlas al entorno de “Producción”.

El segundo ambiente o entorno, es el de “Producción”. Este constituye el Sistema SIGED propiamente dicho. Sobre este ambiente trabajan los usuarios en la operación diaria del Sistema.

Ambos ambientes son necesarios, y es una decisión muy acertada de parte del área de Sistemas de la SGP el haberlos definido e implementado a ambos. Quizás un punto adicional que le agregaría agilidad a la operación del Sistema sería la de implementar un 3° ambiente como sería el de “Capacitación”. De esta forma se podría estar llevando a cabo en forma simultánea las tres acciones normales en el despliegue de un sistema, como son el Desarrollo, Capacitación y Producción. Este último es el estadío actual del sistema SIGED.

Anteriormente se presentaron tres (3) mapas generados con Zabbix. Dos de ellos correspondían a una primera aproximación al modelado y documentación de los dos ambientes antes descriptos. Ver Figura 31 y 32 antes presentadas.

Si bien estos dos ambientes se habían definido a niel de sistemas, es necesario que ambos están bien documentados, y en especial bien identificadas las infraestructuras subyacentes que los soporta. Hay ciertas premisas de diseño, de aislamiento y de configuración; que al ser analizadas y definidas adecuadamente permiten una operación más óptima de la infraestructura y de la disponibilidad de los sistemas en general.

Ahora bien, tomando como base la Tabla 7, se trabajó en el diseño de una nueva tabla empleando el modelo de capas definido y el concepto de Ambiente o Servicio. Es así, que se Definió el ambiente de “Preproducción” como ya se lo mencionó y se lo aisló en la siguiente tabla.

Servicio: PrePROD SIGED					
Nombre	IP	Nombre	Nombre Instancia NOS	IP	Rol /Función
HyperV	10.64.62.135	PREPROD	SIIFprePROD	10.64.62.148	Servidor App
PREPROD	10.64.90.61			(VLAN Educación)	Base de Datos
		DESAFSA		10.64.62.142	Base de Datos
IBM 3650	10.64.62.186	FORMOSA	SERVER10	10.64.62.147	Base de Datos

Tabla 9 – Representación de un Servicio o Ambiente (Preproducción).

Sobre la información simplificada volcada en la Tabla 9, se comenzó a trabajar en conjunto con el personal de Base de Datos, en la definición de nombres y niveles de monitoreo. Estos últimos en base al Modelo de Capas de Monitoreo planteado desde esta consultoría (Tabla 6).

De esta forma se identificaron las distintas capas involucradas, y se definió una primera vista en base a las instancias de las Base de Datos y del Servidor de Aplicación empleado. Es decir, se enfocó en la Capa 7, bajo el ámbito o servicio de “Preproducción”. Así se generó la siguiente tabla.

Servicio: Pre Producción - SIGED			
Nombre Funcional	Nombre Inicial	IP	Rol /Función
Serv. APP	SIIFprePROD	10.64.62.148	Servidor App
Desarrollo	DESAFSA	10.64.62.142	Base de Datos
Prueba	FORMOSA	10.64.62.147	Base de Datos
Producción	BD PREPROD	10.64.90.61	Base de Datos

Tabla 10 – Listado de recursos normalizados asociados al ambiente de Preproducción del SIGED.

La Tabla 10 presenta solo cuatro (4) columnas.

La columna 1 (Nombre Funcional) indica el nuevo nombre asignado al recurso en base a su función dentro del ámbito definido. En este caso se estableció que este nombre representa a la instancia de Capa 7. Como ejemplo, la fila N° 2 Cuyo

nombre funcional es “Desarrollo”, representa la instancia (Capa 7) de la Base de Datos donde se lleva a cabo el desarrollo del Sistema SIGED.

La columna 2 (Nombre Inicial) es el nombre que le asignó el área de Base de Datos inicialmente a la instancia. La columna 3 indica la dirección IP asignada a la MV sobre la cual se ejecuta el Servicio que soporte la instancia. Esta columna merece un análisis más profundo, debido a que este dato es del nivel de Capa 5 según el modelo planteado. Más adelante se revisará esto con mayor profundidad.

Por último, la 4° columna, indiaca el Rol/Función de la instancia.

Como es claro observar, la Tabla 9 es una abstracción de la Tabla 7 original. En ciertos ámbitos técnicos, es necesaria toda la información presenta en la Tabla 7. Pero debería iniciarse un proceso de normalización de dicha información a fin de brindar una base común y coherente con los diseños planteados en este informe. Estos nuevos niveles que se proponen desde esta consultoría forman parte de los procesos normales en los ciclos de desarrollo y vida de las aplicaciones.

En base a la Tabla 10, diseñada en base al modelo propuesto en esta consultoría, se ha diseñado el siguiente mapa en Zabbix, que permite entender el ámbito de “Preproducción” definido. A continuación, se presenta la Figura 34 correspondiente al mapa citado.

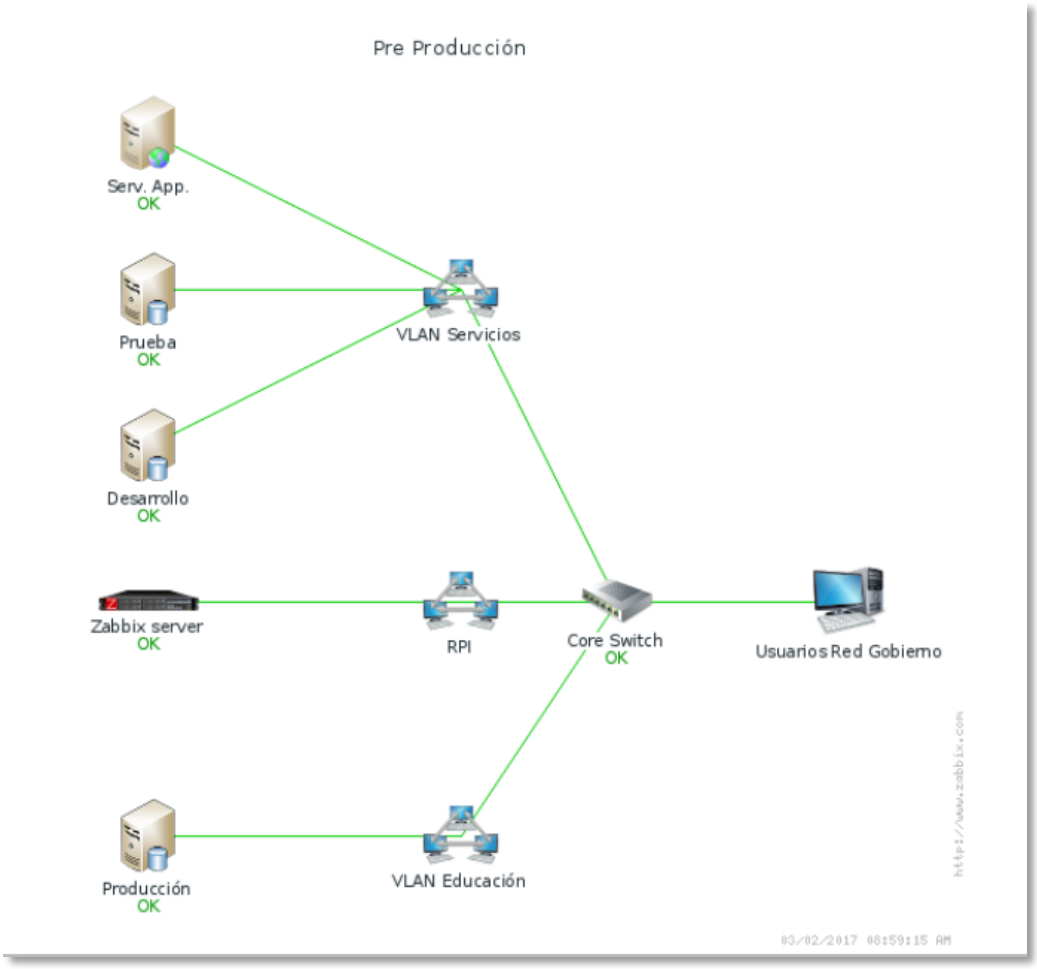


Figura 41 – Mapa del Ambiente o Sistema de Preproducción del SIGED.

Mejoras en las capacidades de Monitoreo

Todo lo planteado hasta el momento a nivel de monitoreo, se ha llevado a cabo bajo un esquema conectividad simple. Es decir, el monitor implementado en este caso Zabbix, corre sobre una instancia de NOS conectado a un red específica.

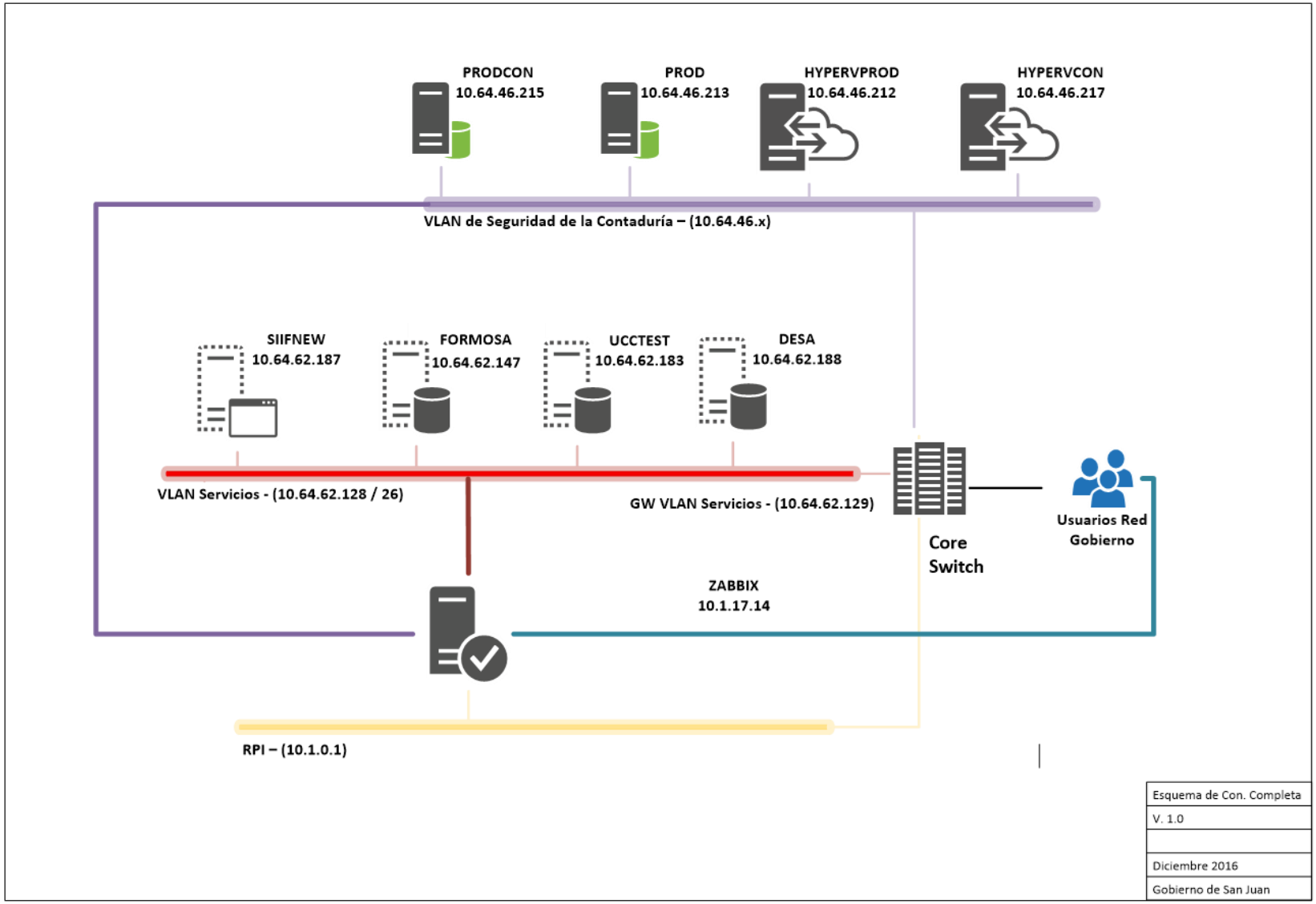


Figura 42 – Layout del esquema de conectividad completo sugerido para la configuración del SGR.

Es necesario comprender que el monitor de red trabaja a nivel de Capa 3 del modelo ISO-OSI en una primera instancia. Es decir que la instancia de NOS donde se ejecuta posee una visibilidad de red, definida por la capacidad de ruteo a nivel de Capa 3.

En el escenario inicial, presentado en la Figura 25, se puede ver al servidor ejecutando el SGR conectado físicamente a la Red Provincial Informática (RPI) cuyo direccionamiento es 10.1.0.0 / 16. Es decir que para que el SGR pueda monitorear los componentes servidores de SIGED debe poder acceso a las VLANs definidas en la red de Gobierno. Esta visibilidad, actualmente se logra a través del ruteo que define el Switch Central de la red del edificio del Centro Cívico. Así la visibilidad de la VLAN de Servicio y de la VLAN de la Contaduría las alcanza el Servidor Zabbix a través del servicio de ruteo que brinda este activo central.

Justamente, la naturaleza de un SGR, o quizás una de sus características principales es detectar funcionamientos anómalos o problemas. En la Figura 25 es bastante simple de ver que todo el tráfico de monitoreo enviado por el monitor de red, para nuestro escenario, es a través del Core Switch o Switch Central. Es decir que si este componente falla, o uno de sus componentes (puertas de enlaces asociadas) pierde la configuración, el SGR queda “ciego”. Es decir, no puede alcanzar ningún destino detrás de este activo. Esto mismo puede presentarse en otros puntos, debido a que todo el tráfico de la red es centralizado.

Por lo presentado en el párrafo anterior, es que se presenta una propuesta de mejora a la conectividad del modelo de monitoreo. Se apunta a ampliar las capacidades de ruteo del SGR, dotándolo de diversas interfaces conectadas a cada uno de los segmentos de red que se desea que monitoree. En la Figura 42 se presenta el esquema de conectividad completo sugerido para la configuración del SGR. Las mejoras presentadas tienen que ver con ampliar las capacidades de ruteo del SGR vinculándolo físicamente a cada uno de los segmentos de red donde existan componentes servidores a monitorear. De esta forma, es posible alcanzar cada uno de los puntos a monitorear (a nivel de direccionamiento IP) por dos vías de ruteo mínimamente. Aparte de la vinculación a la RPI – 10.1.0.1, el SGR debe quedar conectado al segmento de los usuarios de los sistemas (Usuarios red

Gobierno), a la VLAN Servicio – 10.64.62.128 / 26 y a la VLAN de Seguridad de la Contaduría – 10.64.46.x.

Lo presentado en el párrafo anterior, debe ser tomado como un concepto de diseño. Es decir, dotar al monitor de capacidades de conexión redundante hacia un mismo destino.

Servicios TI

Sitio de Intranet – Servicios TI

En función de crear un espacio de publicación que integre todo lo concerniente a la gestión de la Infraestructura TI, se solicitó a la Dirección de Gobierno Electrónico (DGE) dependiente de la Secretaría de la Gestión Pública (SGP), la creación de un micrositio. Este micrositio, a nivel de Intranet de Gobierno, fue denominado Servicios TI (Servicios de Tecnologías de la Información). Su finalidad es la de comenzar a desarrollar un ámbito de publicación unificado de servicios y herramientas tendientes a la administración de la Infraestructura TI de Gobierno. De esta forma en un solo punto de publicación, se propone simplificar el acceso a las soluciones y servicios que se vayan implementando y desplegando. Es fundamental, que este sitio vaya evolucionando en base a los requerimientos y necesidades del ciclo de vida de la Infraestructura TI.

El desarrollo del micrositio estuvo a cargo de la DGE dependiente de la SGP, empleando la plataforma de administración de dominios y subdominios desarrollada por la misma. Desde esta consultoría, se procedió a definir el esquema de contenidos a publicar y la filosofía subyacente del mismo.

Es bueno aclarar que, al momento de la presentación del presente informe, el sitio de Servicios TI estaba en fase de despliegue. Por lo cual las secciones no están del todo definidas, y se trabaja en conjunto con las distintas áreas de la SGP, en ir adoptándolo a los requisitos que se van definiendo.

A continuación, se presenta el diseño inicial implementado:

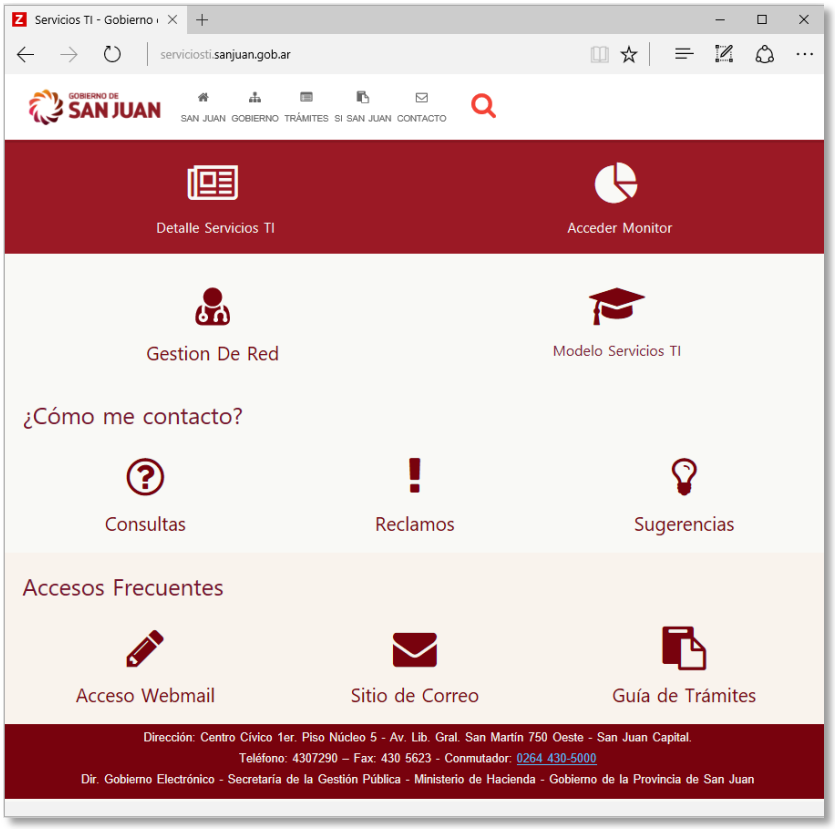


Figura 43 - Diseño inicial micrositio de Servicios TI.

En el mismo hay que identificar dos secciones o áreas funcionales. La primera que es la propia de la Gestión de Servicios TI y una segunda que está definida por la plantilla estándar que ha desarrollado la DGE.

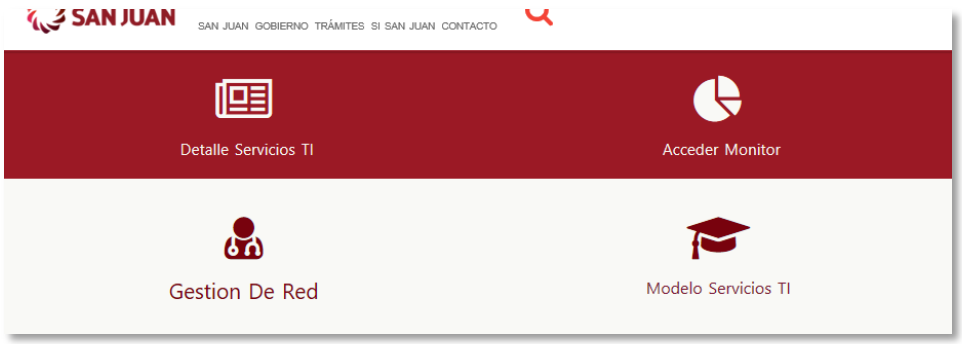


Figura 44 – 2 – 1° Sección - de Gestión de Servicios TI

La primera sección, inicialmente se ha conformado con cuatro íconos o vínculos, los cuales se describe a continuación:

- Detalle Servicios TI: Aquí se propone, publicar una página que describa cada uno de los Servicios Publicados en el sitio de Servicios TI. Adjuntando una descripción y detalle de los mismos.
- Acceder Monitor: Este es el link de acceso a la herramienta de monitoreo propiamente dicha. En este caso sería el acceso a Zabbix como SGR adoptado.
- Gestión de Red. Aquí se debería incluir la tabla de información referencial. Es decir, la información necesaria para gestionar y comprender el Modelo de Monitoreo.
- Modelo de Servicios: Aquí se propone publicar el Modelo de Monitoreo planteado como método de gestión y documentación. Una copia del modelo se presenta a continuación.

La segunda sección corresponde a la plantilla definida y empleada por la DGE. Esta es común a todos los subdominios, la cual se gestiona en la misma plataforma.

Figura 45 - 2° Sección – Información general plantilla definida por Dir. Gob. Electrónico

Desde el ícono “Acceder Monitor” de la 1° Sección, se accede al vínculo que carga la página de validación (“*Sign in*”) del SGR Zabbix. En la siguiente figura, se presenta la pantalla mencionada.

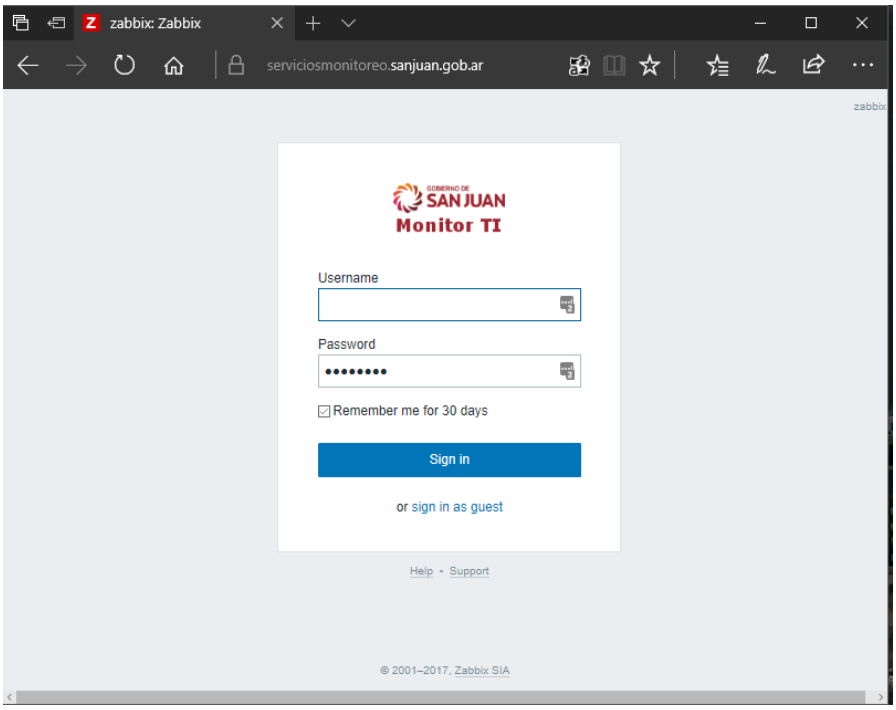


Figura 46 - Pantalla de validación SGR Zabbix.

Esta interface fue personalizada y adaptada a la plantilla empleada en el sitio de Gobierno. Esto con la finalidad de integrarla al diseño y estilos definidos para os sitios del Gobierno de San Juan.

Modelo de Monitoreo propuesto

A continuación, se presenta el borrador final del Modelo de Monitoreo propuesto desde esta consultoría. El mismo se publica en el link que se accede desde el ícono “Modelo Servicio TI” que se encuentra en la primera sección de la página de Servicios TI implementada en conjunto con la DGE, como se mencionó.

Este modelo ha sido puesto a disposición de las autoridades y personal técnico de la SGP, a fin de que se inicie la discusión y adecuación a las necesidades y requerimientos de las áreas de gobierno.

Modelo de Monitoreo de Infraestructura TI

Sistema de Gestión de Infraestructura TI

Secretaría de la Gestión Pública

Marzo 2017

GOBIERNO DE SAN JUAN

Modelo de Monitoreo

En base al estudio realizado en el ámbito del Ejecutivo Provincial, se ha planteado la necesidad de definición de un modelo de monitoreo consensuado y centralizado. Así, desde esta consultoría se trabajó en el diseño de un esquema de monitoreo. El cual se ha planteado como una base para el inicio de un proceso de normalización de la gestión de la infraestructura TI Central de la Secretaría de la Gestión Pública (SGP).

El modelo se define como un conjunto de lineamientos y premisas que sirven como guía y referencia a la hora de administrar la Infraestructura TI. La estructura central del mismo corresponde a la identificación de cada uno de los componentes. Estos componentes pueden ser Software, hardware o Servicios. Y, una vez que es mapeada toda la infraestructura, se comienza a trabajar en la definición y modelado de procesos que completan la gestión de la Infraestructura.

Este modelo, ha sido definido sobre un conjunto de bases teóricas, y es completamente independiente de cualquier herramienta o software en particular. Complementariamente, se llevó a cabo un estudio detallado, y se tomó la decisión que la herramienta de software que puede complementar el despliegue del modelo puede ser el SGR ZABBIX. Pero debe quedar claro que el modelo, vas más allá de la herramienta, sienta las bases teóricas y definiciones, para llevar a cabo la gestión, pero manteniéndose completamente independiente de la herramienta. Quizás en un futuro, sea necesario adecuar la herramienta, o quizás cambiarla por una de mayor evolución. También puede suceder, que, debido a requerimientos, sea necesario adoptar un entorno de monitoreo más amplio. Este, seguramente, debería contemplar la adopción del Modelo aquí enunciado.

Conceptos y Definiciones

A fin de lograr un entendimiento completo del modelo propuesto, se presenta a continuación un conjunto de definiciones y conceptos que son importantes a la hora de su correcta comprensión.

En el Modelo está constituido por 8 capas:

Modelo de Monitoreo – CAPAS			
N°	**Letra**	**Nombre**	**Componentes**
1	I	Instancias	Base de Datos
2	S	Servicios	Aplicaciones, Motor de Base de Datos, Componentes Servidores (Oracle, IIS)
3	O	NOS	Instancia de NOS, Servicios de SO
4	V	MV	Memoria, Disco, NICs Virtuales
5	H	Hypervisor	Software, Servicios
6	A	Anfitrión	Modo no Nativo
7	F	Físico/Hard	NICs Físicas, Memoria, Discos
8	C	Conectividad	Activos, Gateways, Firewalls

Tabla A – Modelo de Capas

Las 8 capas presentadas, pretenden precisar detallada y claramente la totalidad de la infraestructura TI asociada. Esta definición se lleva a cabo mediante la aplicación del método de estratificación. Es decir que se adopta el modelo de capas, a fin de intentar establecer límites y facilitar el entendimiento del modelo. Estos límites involucran el aislamiento de los componentes, agrupándolos en conjuntos bien definidos y acotados. Estos conjuntos permiten, complementariamente, asignar responsabilidades y facilitar la especialización de los agentes asignados a gestión y administración de cada uno. Así, de forma correlacionada con el modelo, se puede iniciar un proceso de definición de roles con sus respectivas responsabilidades. Lo anterior, enfocado en un proceso de restructuración de áreas e incumbencias, podría agilizar y consolidar la normalización de las áreas relacionadas. Y paralelamente

ayudar a la definición de los responsables de la gestión y operación de la Infraestructura TI. Esto último se describirá más adelante en las siguientes secciones.

Este modelo contempla lo asociado y aportado por entornos virtualizados. Es decir que en su concepción se consideró la modelización de estos ambientes. En el caso del Gobierno de San Juan, se ha iniciado un proceso consolidación total de la Infraestructura TI. Por lo cual la adopción del modelo aquí enunciado aplicaría completamente.

Otro concepto importante, es que el modelo se despega, es independiente, de las unidades de cómputo. Entendemos por unidades de computo todo aquel equipamiento que tiene la capacidad ejecutar un Sistema Operativo de Red. El ejemplo más simple de una Unidad de Computo sería una CPU tradicional. Es decir, es hardware con su Sistema Operativo correspondiente (con capacidad de cómputo, memoria, almacenamiento y conectividad) que pueden brindar servicios TI y ejecutar aplicaciones. Y, en un nivel de mayor complejidad y capacidad podemos presentar un sistema de cómputo unificado como sería un sistema Flex de IBM por ejemplo. En este último se pueden ejecutar múltiples máquinas virtuales, las cuales albergan y ofrecen cientos de Servicios TI y ejecutan infinidad de aplicaciones.

En estos dos entornos, desde el más simple (Unidad de Cómputo), hasta un sistema de Computo Unificado, lo importante es identificar cada uno de los componentes implementados. Entendemos por componente, desde el punto de vista del modelo, a aquella unidad indivisible a nivel de operatividad. Es decir, que un componente define una unidad que, según el modelo, nos interesa ser analizada como un todo. Ejemplos de componentes pueden ser:

- Una instancia de una Base de Datos (o Base de Datos propiamente dicha).
- Un motor de Base de Datos: nos interesa saber si el motor opera en forma correcta. Si bien deben estar activos numerosos servicios del Sistema Operativo para que el motor esté operativo, desde el punto de vista del modelo se considera que el Motor de Base de Datos como un todo, es decir un único componente.
- El Sistema Operativo de Red (NOS por sus siglas en Ingles). Un Sistema Operativo está compuesto por un gran número de programas, servicios,

configuraciones, etc. Pero, según la definición del modelo, se lo debe considerar como una unidad indivisible.

De lo anterior, se desprende que para que un componente esté operativo, deben operar satisfactoriamente numerosos subcomponentes. Esto determina un concepto asociado que es el nivel de severidad de las fallas o incidentes que manifiestan los elementos (subcomponentes) que constituyen un componente. Profundizar en este concepto, en esta etapa de la definición del modelo, atentaría contra el entendimiento del mismo. Por lo cual, más adelante, se trabajará detalladamente en definir este 2° nivel dentro de cada uno de los componentes.

Una posibilidad válida para determinados escenarios es que no sea necesario modelar o identificar la totalidad de las capas para cada una de las Unidades de Cómputo. Un ejemplo de lo anterior es el caso de la implementación del Hypervisor Tipo 1 (modo nativo), en el cual no se emplea un NOS como anfitrión del Hypervisor. Es decir que la Capa 6 no estará presente en este caso. O también, es posible modelar y monitorear la Infraestructura sin incluir la Capa 8 – Conectividad. Si bien esto no es para nada aconsejable, es perfectamente factible desde la versatilidad del Modelo.

Otro concepto importante es el de la “dependencia” de componente de distintas capas. Esto refiere a que determinados conjuntos de componentes dependen operativamente de un componente de la capa siguiente. Un ejemplo claro es la dependencia entre instancias de Bases de Datos (Capa 1 – Instancia) y el motor de la Base de Datos (Capa 2 – Servicios). Si el Motor de BD no está operativo, afectará al conjunto de instancias de Bases de Datos que estén ejecutándose sobre ese Motor de BD. Una falla en un componente de la Capa 2, seguramente impactará en la operatividad de uno o más componentes de las capas menores. En este caso, serían componentes de la Capa 1 – Instancias.

Es común entender que los componentes conforman un conjunto indivisible, asociados a un contenedor físico que puede entenderse como un CPU o Unidad de Computo como ya se definió anteriormente. Así, en una CPU podemos encontrar componentes para cada una de las capas definidas. Pero el modelo propone dejar de lado este preconcepto. Y entender la Infraestructura TI como un conjunto de

componentes, aislados e independientes, a los cuales se los identifica dentro de en una determinada Capa del Modelo.

Es bueno aclarar que el modelo que se propone tiende a definir un estándar inicial, el cual sería aconsejable que sea evolucionado conforme evolucionen los requerimientos y la madures de la infraestructura asociada. Se toma como práctica acompañar las definiciones con ejemplos tendiendo a aclarar el alcance y los conceptos asociados del mismo.

Definición de las Capas

Las capas definidas en el Modelo son 8:

Capa 8: Conectividad (C). Esta capa engloba todos los componentes asociados con la conectividad física a nivel de red informática. Ejemplos de esta capa serían, switchs, routers, activos administrables y demás componentes involucrados con la red física propiamente dicha.

Capa 7: Física (F). Esta capa agrupa los componentes Físicos o Hardware de la Infraestructura. Aquí estarían involucrados desde una CPU individual hasta una infraestructura de cómputo unificada como sería un sistema Flex o Blade de IBM como ejemplo (Unidad de Cómputo). Esta capa también debería abarcar el hardware asociado al almacenamiento. (Storage).

Capa 6: Anfitrión (A). Esta capa está relacionada con el tipo de hypervisor implementado. En el caso de ser el Tipo 2 (No Nativo o Hosted), esta capa modela o representa el Sistema Operativo de Red empleado (en inglés Network Operating System - NOS). El Tipo 2 refiere a que el hypervisor se instala como un servicio de un Sistema Operativo Anfitrión. Este es el caso de las implementaciones del hypervisor Microsoft HyperV que tiene actualmente implementada la Contaduría General de la Provincia del Ministerio de Hacienda. En el caso de implementar hypervisores del Tipo 1, esta capa no debería ser modelada.

Capa 5: Hypervisor (H). Aquí deben incluirse todas las propiedades o servicios relacionados con el hypervisor, necesarios para definir cada uno de los

componentes. Es decir que esta capa asocia todo lo referente con la operación del componente de software hypervisor.

Capa 4: Virtual (V). Esta capa refiera a las MVs (Máquinas Virtuales). Aquí se deben monitorear todos los servicios y propiedades asociados a la operación de cada una de las Máquinas Virtuales que conforman la Infraestructura. Cada una de las MVs modelada correspondería a un componente de esta capa.

Capa 3: Operativo (O). En esta capa se deberían incluir todos los servicios y propiedades que tengan relación o pertenezcan a las instancias de cada uno de los NOS. Estos Sistemas Operativos, pueden ser instancias ejecutando sobre Máquinas Virtuales, o sobre hardware físico propiamente dicho. Así un NOS instalado sobre un servidor simple o una CPU debería estar monitoreado en esta capa. Hay que tener bien claro la diferencia entre esta Capa (Capa 3) y la Capa 6 – Anfitrión. Esta capa involucra los NOS sobre los cuales se despliegan aplicaciones y Servicios, mientras que la Capa 6 refiere a los NOS empleados como anfitriones de un hypervisor concretamente.

Capa 2: Servicios (S). Esta capa debe abarcar todos los componentes de software relacionados con la capa de servicios. Dos ejemplos concretos de lo que se debe monitorear en esta capa es el servicio Web (o httpd) y el Motor de Base de Datos. En el primer caso sería todo lo necesario para que el servicio de publicación Web esté operativo. En el caso de las aplicaciones como es el SIGED que ejecuta la Contaduría sería todo lo referido al IIS (Internet Information Services). Es decir, que servicios y programas son necesarios que estén ejecutándose para que el servicio sea correctamente entregado. Cada Servicio corresponde a un componente. Otro ejemplo muy gráfico, es todo lo relacionado a la operatividad de un motor de Base de Datos. Así en el caso de la Contaduría General de la Provincia, serían los servicios necesarios para que esté operativa cada instancia del motor de la Base de Datos Oracle.

Capa 1: Instancias (I). Esta capa agrupa todo lo relacionado a las instancias de los servicios o aplicaciones específicos. El ejemplo más claro de componentes de esta capa son las distintas instancias de Bases de Datos que están ejecutando.

Se le ha asignado una letra a cada una (ver Tabla A), la cual corresponde a la inicial del nombre con el que se ha bautizado la Capa. Uniendo las iniciales en el orden ascendente de la numeración asignada, se obtiene la sigla con la que se bautizó el modelo: ISOVHAFC. Otra denominación propuesta, es la de separar la capa 8 (la Capa de conectividad). Esta capa actualmente es administrada y monitoreada por personal de la Dir. de Conectividad y Telecomunicaciones, por lo cual quizás no sea conveniente incorporarla en el esquema de modelado implementado en una etapa inicial. Así se plantea la variante ISOVHAF + C. Lo ideal y propuesto desde esta consultoría es que se incorporaren y modelen la totalidad de las capas. Es decir, las 8 capas definidas.

Propuesta de Denominación

Propuesta

El siguiente modelo presentado, es tan solo una propuesta de nomenclatura. Se propone como base de discusión inicial, a fin de ir evolucionándola hacia los requerimientos de la SGP. Si bien ya se ha realizado un análisis detallado y profundo de los requerimientos de la Secretaría, el ponerlo a consideración de las distintas áreas involucradas permitirá llevar el modelo a un estadío de madurez adecuado a la cultura de la organización.

Definiciones

Inicialmente se estableció una plantilla base para encuadrar o semiestructurar la nomenclatura a emplear. Se define una nomenclatura de una palabra de 4 secciones, la cual se presenta a continuación:

[Capa] - [Denominación] - [Función] - [Ámbito]
[1] - [3 a 8] - [3] - [3]

Se aconseja como premisa inicial que cada una de las secciones, esté compuesta por 3 caracteres y que sean separados por un guion. La excepción de lo anterior sería la primera sección que se propone esté constituida por un solo carácter (alfabético).

Es decir que la palabra, idealmente, debería tener una longitud total de 10 caracteres (3 caracteres x 3 secciones = 9 caracteres, más 1 carácter de la primera sección). Complementariamente, para incorporarle un orden visual, se aconseja emplear 3 guiones de separación, lo cual daría una longitud ideal de 13 caracteres.

De esta forma se obtendría una palabra simple de manipular, recordar y con la suficiente definición en la representatividad del componente.

La 2° sección “Denominación” se propone tenga una longitud inicial de 3 caracteres. Pero bien, debido a la amplia variedad de componentes que puede llegar

a modelarse, se define que la longitud de esta sección pueda crecer hasta 8. Esta particularidad es a fin de darle capacidad de descripción a los nombres a emplear, sin perder la característica de fácil lectura y claridad de los mismos. Es bueno aclarar que nombres muy extensos, dificultan la manipulación y memorización.

Descripción de las Secciones

A continuación, se procede a describir cada una de las secciones definidas en el modelo.

1° Sección - **Capa** – Esta sección corresponde a la identificación de la capa a la cual pertenece el componente a modelar. Se ha definido que esta sección posea un (1) solo carácter, el cual corresponde a la letra inicial de la capa correspondiente.

2° Sección – **Denominación** – Esta sección también podría llamarse "Nombre". Es decir que aquí debe describirse el componente específicamente. Se pueden llevar a cabo preacuerdos, y es aconsejable que así suceda, respecto al uso de cada una de las secciones.

3° Sección – **Función** - Esta sección debe describir que función tiene asignado cada uno de los componentes. Debe describir su rol técnico, funcional. Esta sección debe estar relacionada con la siguiente. Es decir, que se debe especificar su función dentro del ámbito.

4° Sección – **Ámbito** – Esta sección define que se describa el alcance o un espacio definido respecto de la funcionalidad del componente. El ámbito debe ser empleado a fin de agrupar componentes que desarrollen funcionalidades relacionadas.

Más adelante, en las siguientes secciones, se presentará una serie de ejemplos con la finalidad de facilitar el entendimiento y la aplicación del modelo.

Adicionalmente, se han definido dos conceptos complementarios que pueden ser empleados para enriquecen la capacidad descriptiva del modelo. Estos serían la "Serie" y la "Ubicación".

Conceptos Adicionales

Conceptos Adicionales	Detalle
[Serie]	Representa la enumeración de la secuencia de instancias de un mismo componente.
[Ubicación]	Se empleará en especial en la capa de 7-Físcia. Para detallar la ubicación de los componentes físicos.

Tabla B – Conceptos Adicionales

Serie: La Serie refiere a incorporación de una serie numérica en alguna de las secciones, a fin de ayudar a la identificación unívoca del componente. Estas series normalmente son empleadas para la identificación o nombrado de componentes que constituyan una secuencia sin propiedades claras para ser descriptas. Un ejemplo de esto, pueden ser los activos de conectividad. Los cuales al ser agrupados dificultan su individualización.

Ubicación: La Ubicación refiere a la incorporación de un indicador o valor que represente el lugar físico del componente. Ejemplo de esto puede ser, un N° de racks, Nombre o N° de Sala, N° de Piso, Nombre de edificio o similar. Suele emplearse para componentes de la capa física o de conectividad.

A continuación, se presentan un par de ejemplo del empleo del parámetro de ubicación.

Por ejemplo, en el caso de servidores, storage o UPSs rackeables, una buena forma de emplear la ubicación es haciendo referencia al Rack en el cual está instalado, y luego a la Unidad. Así, por ejemplo, en los racks que posee la DPI actualmente, los cuales son de 42 unidades la mayoría, se podría referenciar de la siguiente manera:

- Emplear las unidades inferiores para el equipamiento más pesado, como pueden ser las UPSs.
- Emplear la unidad del medio, o central, para ubicar la consola de administración.
- Y las restantes unidades para la ubicación de los componentes servidores.
- El Storage, se puede tomar como norma ubicarlo, inmediatamente sobre las UPSs.

Lo anterior determina ciertos lineamientos respecto a la distribución física, que contribuye con la normalización.

Complementariamente, se podrían etiquetar los Racks con una letra cada uno. Rack A, Rack B, y así sucesivamente. Considerando, por supuesto, la cantidad de los mismos. De ser necesario se podría ampliar el rango apelando al empleo de 2 letras para tal fin. Así hablaríamos de Rack AA, Rack AB, etc.

Al indicar la ubicación de un componente, como puede ser un servidor de una unidad ubicado en la unidad 10 del Rack A, nos referiríamos como: Servidor A10.

Otros ejemplos serían, Consola B24, UPS C40, Storage B34

De esta forma es fácil referenciar un componente, y particularmente simplifica sensiblemente la ubicación y gestión de hardware en ambientes de alta densidad de equipamiento. Y en especial si el trabajo es realizado por equipos de trabajo.

Esta denominación debe ir acompañada por un proceso continuo y minucioso de documentado en herramientas de gestión asociadas. Más adelante se analizará este tema en forma detallada.

Ejemplos de Denominación

Ejemplos:

Nombre	Significado
I-WAP-SGE-PRO	Componente de la capa Instancia, WebAplication (Aplicación Web), del Sistema de Gestión de Expedientes, en el Ambiente de Producción

S-IIS-SGE-PRO	Componente de la Capa de Servicio – Servicio del Internet Information Server – del Sistema SIGED – en el Ambiente de Producción.
H-DPI01-ESX-PRO	Componente de la Capa de Hypervisor – Hypervisor DPI N° 1 – VMWare ESXi – en la Infraestructura de Producción.
S-ZAB-SGR-DPI	Componente de la Capa de Servicio – Zabbix – Sistema de Gestión de Redes - Entorno Operativo en la DPI.
F-FLE-N01-PRO	Capa Físico – Flex System – Nodo 1 – Infraestructura de Producción

Tabla C – Ejemplos de Denominación

Denominaciones Propuestas para soporte del Sistema SIGED

A continuación, se ha desarrollado un conjunto de ejemplos de aplicación de la nomenclatura propuesta por el modelo.

Ambiente de Desarrollo – Sistema SIGED				
Capa	Desarrollo	Producción	ServApp	Detalle
1	I-BDD-SGE-DES	I-BDP- SGE-DES	I-SGE-WAP-DES	DES = Ambiente de Desarrollo
2	S-O2D-SGE-DES	S-O1P- SGE-DES	S-SGE-IIS-DES	
3	O-W2P- SGE-DES	O-W1P- SGE-DES	O-SGE-WAP-DES	
4	V-BDD- SGE-DES	V-BDP- SGE-DES	V-SGE-WAP-DES	
5	H-DPI01-DES-ESX	H-CON02-HYP-DES	H-CON01-HYP-DES	HyperVisor – Contaduría 01 – Desarrollo – Versión HyperV
6		A-W02- SGE-DES	A-W01 SGE-DES	
7	F-FLE-N01-PRO	F-S01-IBM-CON	F-BCS-B01-CON	BCS (Blade Chasis S)
8				

Tabla D – Denominaciones Propuestas para el Ambiente de Desarrollo (SIGED)

Ambiente de Producción - Sistema SIGED				
Capa	Desarrollo	Producción	ServApp	Detalle
1	I-BDD- SGE-PRO	I-BDP- SGE-PRO	I-WAP- SGE-PRO	PRO = Ambiente de Producción WAP = Web Application
2	S-O2D- SGE-PRO	S-O1P- SGE-PRO	S-IIS- SGE-PRO	
3	O-W2D- SGE-PRO	O-W2P- SGE-PRO	O-W1P- SGE-PRO	
4	V-BDD- SGE-PRO	V-BDP- SGE-PRO	V-WAP- SGE-PRO	
5	H-DPI01-PRO-ESX	H-CON02-HYP-PRO	H-CON01-HYP-PRO	
6		A-W02 SGE-PRO	A-W01 SGE-PRO	
7	F-FLE-N01-PRO	F-BCS-B01-PRO	F-BCS-B01-PRO	

8				

Tabla E – Denominaciones Propuestas para el Ambiente de Producción (SIGED)

Documentación Referencial

Es aconsejable, mantener un archivo asociado o quizás una Base de Datos debidamente publicada en una intranet, con la finalidad de mantener documentado los nombres asignados a cada uno de los componentes. Y fundamentalmente como referencia de los usuarios del Modelo, en los primeros tiempos del proyecto de implementación. En la medida que cada uno de los usuarios del mismo vaya familiarizándose, o use cotidianamente el modelo, se debería volver bastante natural el esquema de nomenclaturas.

Esta documentación debería enriquecerse con la mayor cantidad de información posible, que facilite la interpretación y entendimiento de las políticas y directrices que se emplearon. En especial, como ya se dijo, en las fases iniciales de la implementación del mismo.

Así, por ejemplo, se puede plantear como base una tabla, de cuatro columnas que describan la nomenclatura. Y se podrían agrupar por los diferentes ámbitos que se definieran. Esto último a fin de simplificar la administración de la Infraestructura. La adecuada definición de los diferentes ámbitos simplifica notablemente la administración del seguimiento de componentes. En especial cuando se monitorea un gran número de los mismos.

Ambito – [Producción]			
Nomenclatura	**Referencia**		
	Denominación	Función	Ámbito
F-FLE-N01-PRO	Sistema FLEx	Nodo 01	PROducción
S-IIS-SGE-PRO	Internet Information Server	Sistema de Gestión de Expedientes	PROducción
O-BO1-SI-PRO	Base de datos Oracle 1	Sistema Integrado	PROducción

Tabla F – Propuesta de Documentación Referencial

Esta tabla, también puede ser transformada en una Base de Datos, con la finalidad de poder administrar mejor el contenido. En forma complementaria, se podría relacionar o vincular con un Sistema de Administración de Activos (en inglés *Asset Management*) o Sistema similar de gestión de infraestructura TI.

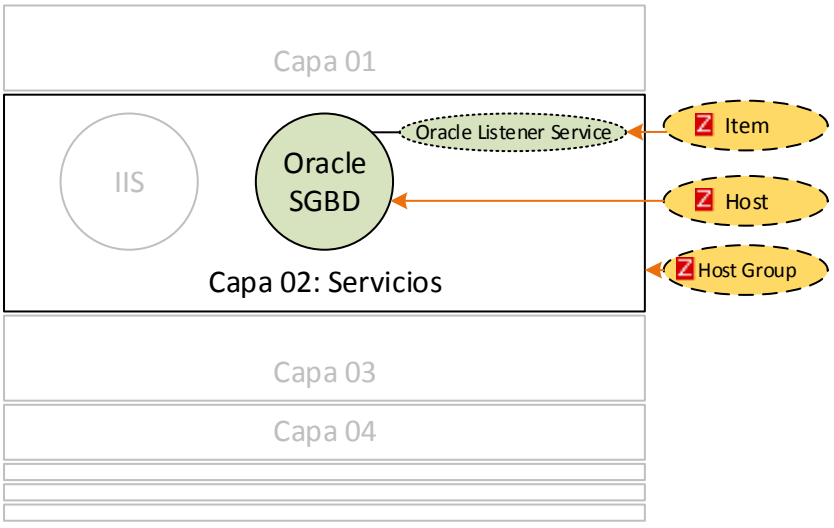
Herramienta o Software a emplear

Software empleado

El producto empleado para la implementación del Modelo propuesto, como ya se mencionó, es Zabbix. Es un Sistema de Gestión de Red (SGR) muy conocido y muy bien conceptuado. Es importante comprender que un aspecto relevante de la implementación de este Modelo de Monitoreo es lograr la correcta adaptación de la herramienta al modelo planteado.

A continuación, veremos ciertas características particulares de la herramienta de software empleada.

Implementación del Modelo en Zabbix



Host Group: representa una capa del modelo. Puede contener varios Host.

Host: representa un componente de una capa del modelo. Por ejemplo: el SGBD Oracle.

Ítem: representa cada elemento necesario para determinar si el componente de la capa se encuentra operativo (Host). Por ejemplo: para el componente “Oracle SGBD”, se debe determinar su funcionamiento dependiendo si el servicio “Oracle Listener Service” se encuentra activo.

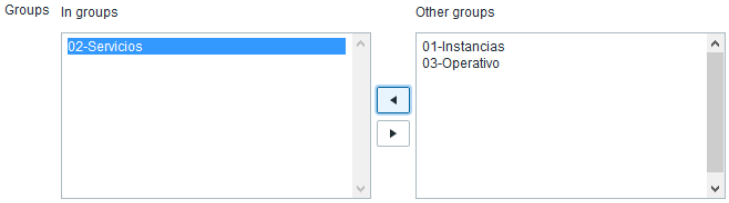
Nota: *Es fundamental una coordinación entre el área de monitoreo y el área técnica específica a fin de determinar que propiedades deben ser configuradas para*

determinar la operatividad de cada uno de los Hosts. Esto tiene una fuerte relación con los niveles de severidad que puede manejar Zabbix.

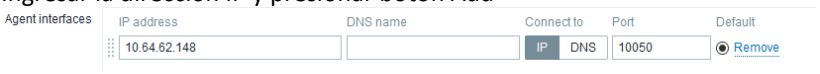
Como agregar un componente de una capa y elementos a Zabbix:

- Crear un host que representará al componente en Configuration > Hosts.
- Ingresar el nombre del componente:

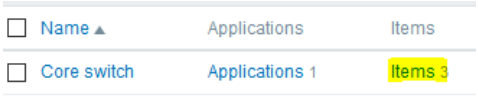
- Seleccionar la capa a la que se agregará:



- Ingresar la dirección IP y presionar botón Add

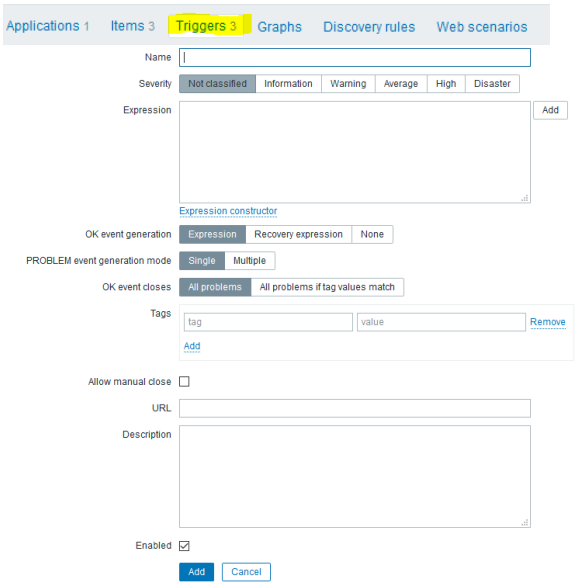


- Se procede a cargar cada ítem que representará a un elemento a monitorear del componente



- Se ingresa el nombre y se configuran los demás parámetros de acuerdo a qué dato se quiere obtener (dependerá de la capa a la que pertenezca el componente)

- Por último se crean los Triggers para generar las alertas cuando los valores de los ítems superen un umbral:



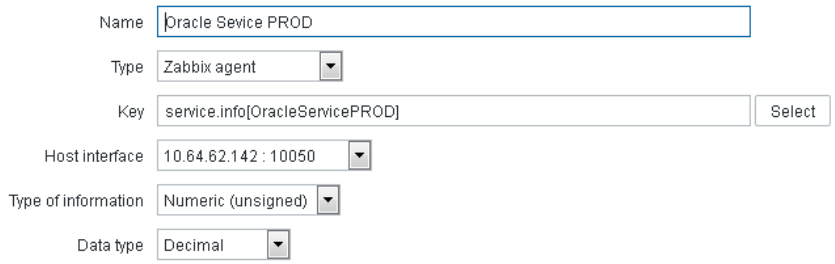
Ejemplos de elementos de un componente de capa implementado en Zabbix

Capa instancia (1)

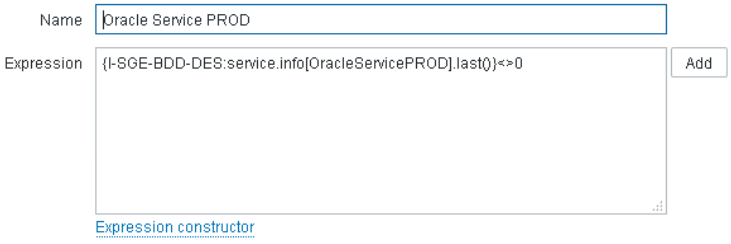
Monitoreo de una instancia de base de datos de Oracle. Para tal caso, se obtiene el estado del servicio correspondiente a la instancia: “OracleServicePROD”. Se requiere del funcionamiento del agente Zabbix en el host.

Para el host que representa el componente, agregar un nuevo ítem y hacer:

- Cargar el nombre del ítem
- Elegir el Type Zabbix Agent
- Key es el establecido por Zabbix para obtener el estado de un servicio.



- Luego se crea un Trigger para mostrar la alerta cuando el estado del servicio sea distinto de “Up” mediante la expresión:

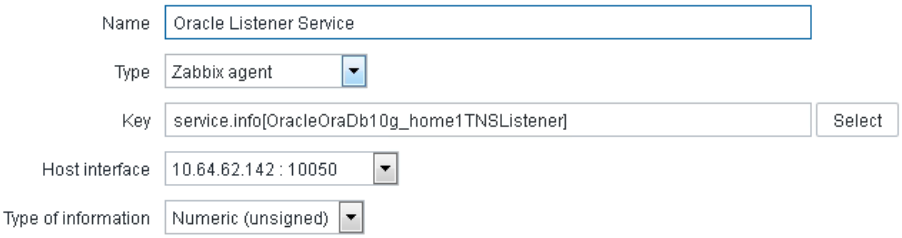


Capa Servicio (2)

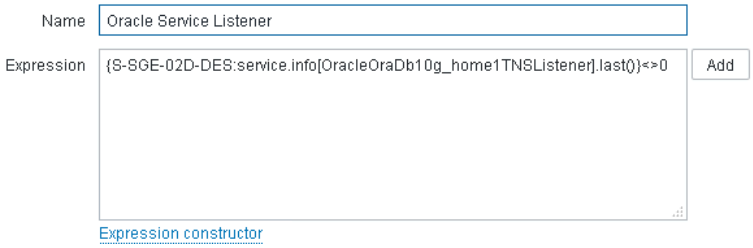
Monitoreo del servicio correspondiente a un SGBD Oracle. Para tal caso, el monitoreo se realizara obteniendo el estado del servicio correspondiente: “OracleOraDb10g_home1TNSListener”. Se requiere del funcionamiento del agente Zabbix en el host

Para el host que representa el componente, agregar un nuevo ítem y hacer:

- Cargar el nombre del ítem
- Elegir el Type Zabbix Agent
- Key es el establecido por Zabbix para obtener el estado de un servicio.



- Luego se crea un trigger para mostrar la alerta cuando el estado del servicio sea distinto de



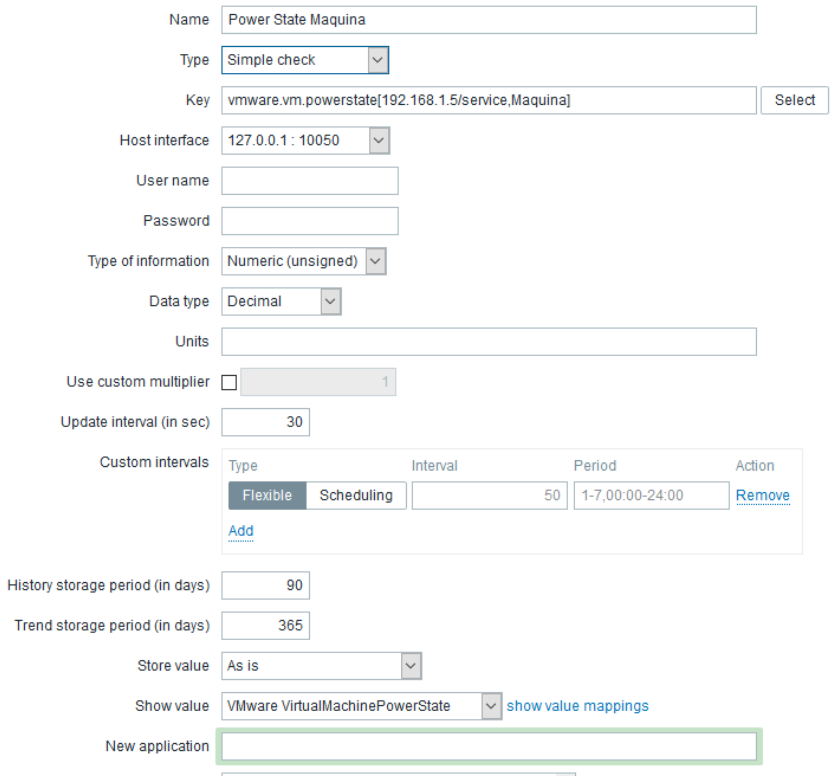
"Up" mediante la expresión:

Capa MV (4)

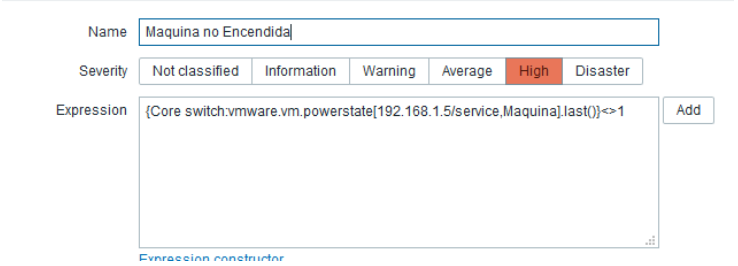
Monitoreo del estado (encendido, apagado, suspendido) de una máquina virtual de VMWARE. Cargar el nombre del ítem

Para el host que representa el componente, agregar un nuevo ítem y hacer:

- Elegir el Type Simple Check
- Utilizar Key vmware.vm.powerstate para obtener el estado de una máquina virtual, indicando la URL del servicio de vmware y el hostName de la máquina virtual
- El parámetro "ShowValue" debe ser: "Vmware VirtualMachinePowerState"



- Luego se crea un Trigger para mostrar la alerta cuando la máquina virtual cambie de estado

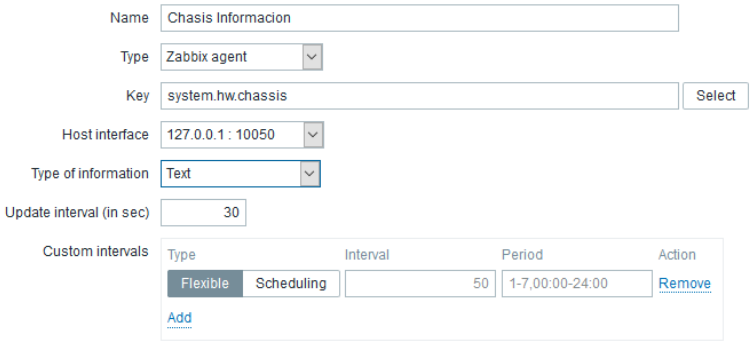


Capa Física (7)

Monitoreo de información de chasis.

Para el host que representa el componente, agregar un nuevo ítem y hacer:

- Cargar el nombre del ítem
- Elegir el Type Agent Zabbix
- Key: system.hw.chassis
- Type of information: Text



Implementación de modelo ISOVHAFC en Zabbix

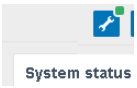
Una manera de implementar el modelo sin agregar complejidad a la operación y mantenimiento de Zabbix es crear un Host para cada componente de cada una de las capas que define el Modelo ISOVHAFC. Los ítems se corresponderán con las propiedades del componente a monitorear según la capa

En cada host, sobre el que corren las aplicaciones o servicios a monitorear, se debe instalar un agente de monitoreo propio de Zabbix, el cual le proporcionara información sobre el estado de cada elemento. Para el caso de Hypervisores, la forma de monitorear variará según si se encuentra funcionando de forma nativa o no.

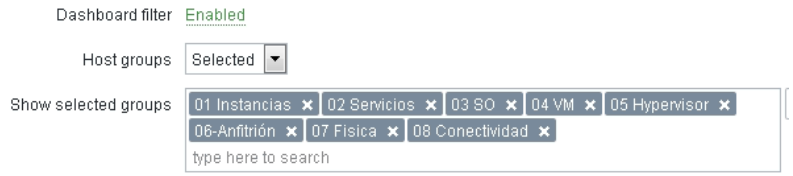
Para el primer caso, en modo nativo, se debe instalar el agente de Zabbix directamente en el Hypervisor corriendo como un servicio adicional. Para el modo no nativo, se debe instalar el agente en el sistema operativo (Anfitrión) que soporta el servicio de Hypervisor.

Para el armado de las capas, se procede a crear grupos de Host, cuyos nombres se corresponderán con los nombres de las capas. Luego se deben incluir los Host que correspondan.

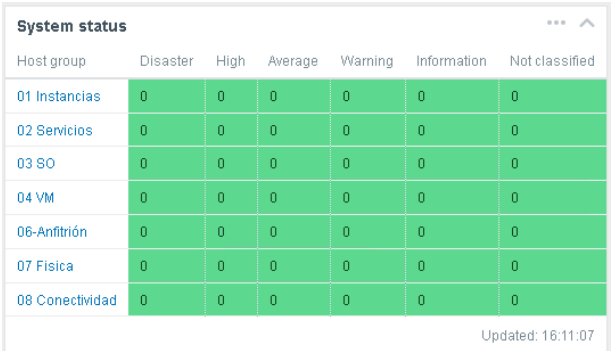
Para la visualización del estado de cada capa, en el *dashboard* de Zabbix, se despliega el control *System Status* y se configura para que muestre solo el estado de las capas y no de los demás grupos de host. Mediante el botón de configuración del *dashboard* se accede a la interfaz de filtrado:



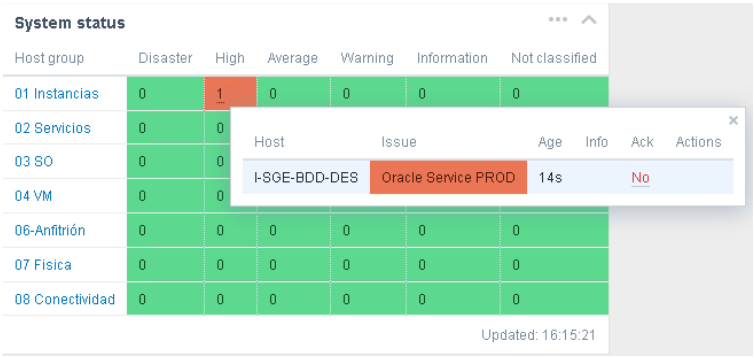
Se habilita el filtrado y se seleccionan los grupos correspondientes a las capas.



El control System Status queda de la siguiente forma:

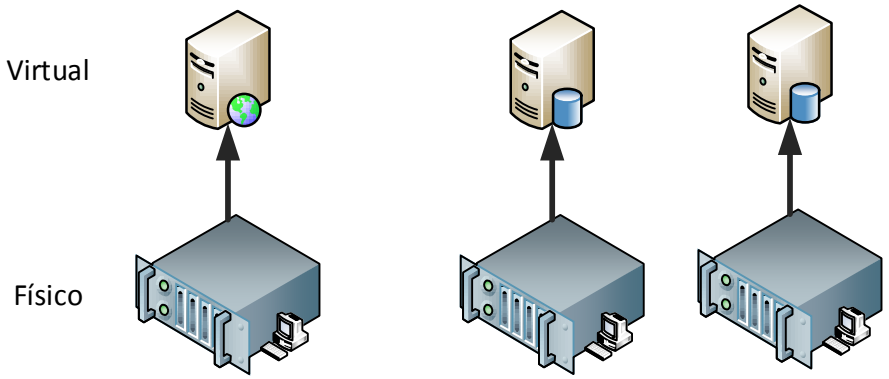


Cuando ocurre un problema, se marca en estado de error la capa correspondiente junto con el número de elementos que fallaron, mostrando además el detalle de cada uno.



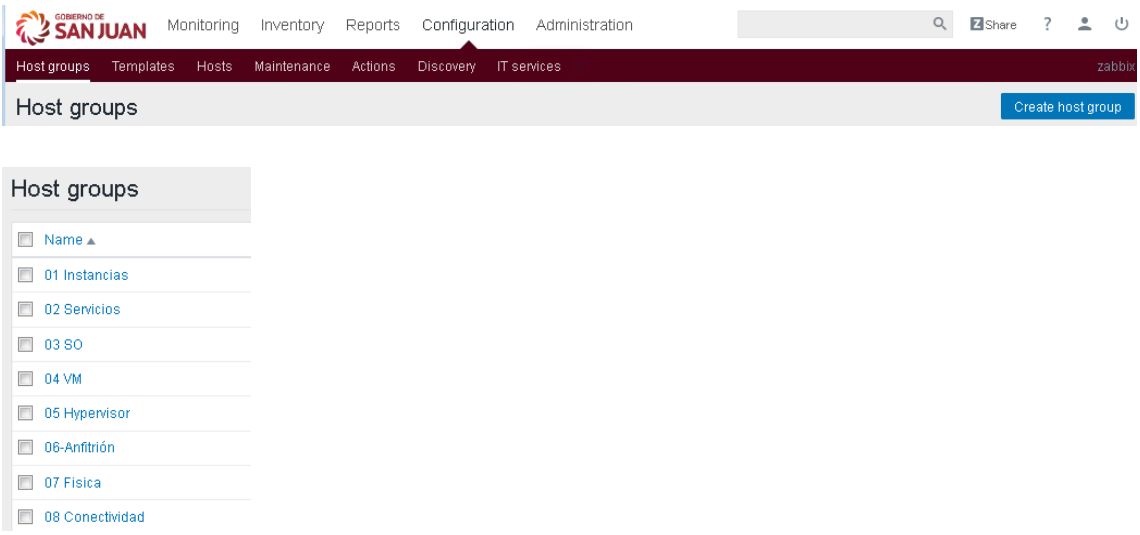
Monitoreo del ambiente de Preproducción de SIGED

Para el monitoreo del entorno de desarrollo de SIGED, el cual comprende de tres máquinas virtuales y tres físicas: cada una de las físicas tiene un Hypervisor que almacena y gestiona una de las máquinas virtuales del sistema. De las tres virtuales, una contiene el servidor de aplicaciones que corre la aplicación SIGED y las otras dos tienen un motor de Base de Datos Oracle.

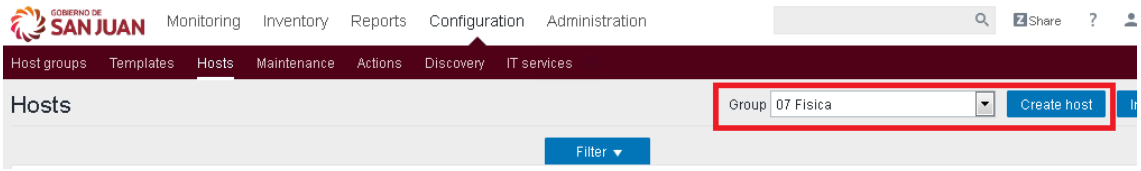


Por lo tanto, se implementa el monitoreo de los componentes de SIGED aplicando el modelo ISOVHAFC de la siguiente manera:

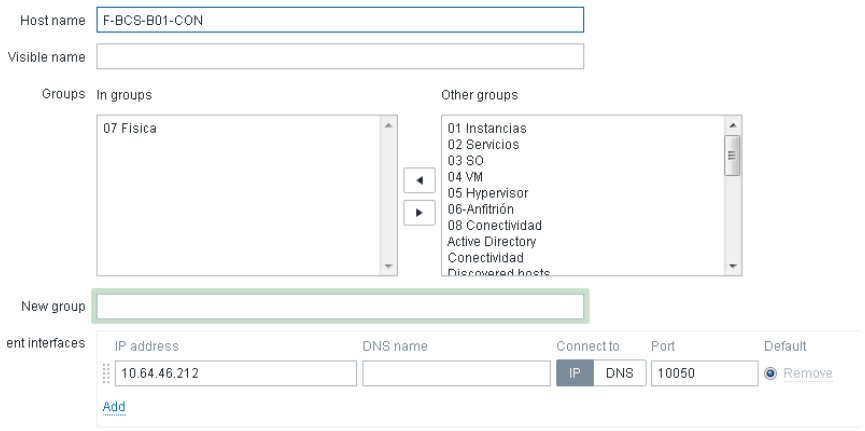
Se crean 8 grupos de hosts correspondientes a cada una de las capas del modelo, desde el menú Configuration > Host Groups



Para cada capa se crean los hosts que representan los elementos a monitorear de cada capa. En el menú Configuration > Hosts, se elige el Group que representa la capa y se solicita Crear Host



Se asigna el nombre basado en un esquema de nombres definido, la dirección Ip y se indica en qué capa va a estar.



Capa Instancias (01)

Se monitorea la instancia de IIS que corresponde con la aplicación SIGED y la base de datos especifica que usa. Para el primero se prueba la apertura del puerto correspondiente a SIGED y la devolución del código de respuesta HTTP. Para la base de datos de SIGED en Oracle, se monitorea el funcionamiento del servicio que corresponde a la instancia (OracleServicePROD)

Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface
I-SGE-BDD-DES	Applications	Items 1	Triggers 1	Graphs	Discovery	Web	10.64.62.142: 10050
I-SGE-BDP-DES	Applications	Items 1	Triggers 1	Graphs	Discovery	Web	10.64.90.61: 10050
I-SGE-WAP-DES	Applications	Items 1	Triggers 1	Graphs	Discovery	Web	10.64.62.148: 10050

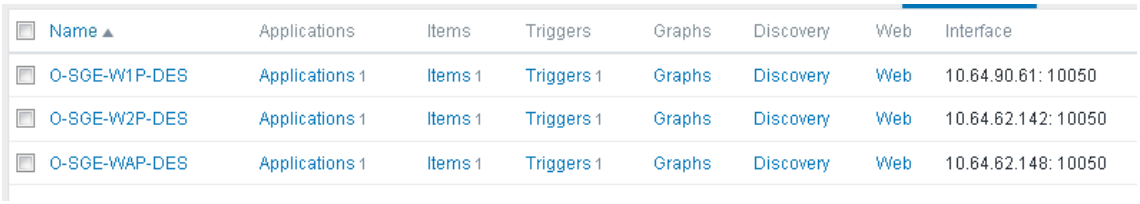
Capa Servicios (02)

Para los servicios de servidor de aplicación de SIGED se verifica el funcionamiento del servicio de IIS y para los servicios de SGBD se monitorea el servicio “OracleOraDb10g_home1TNSListener”

Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface
S-SGE-01P-DES	Applications	Items 1	Triggers 1	Graphs	Discovery	Web	10.64.90.61: 10050
S-SGE-02D-DES	Applications	Items 1	Triggers 1	Graphs	Discovery	Web	10.64.62.142: 10050
S-SGE-IIS-DES	Applications 1	Items 1	Triggers 1	Graphs	Discovery	Web	10.64.62.148: 10050

Capa Operativo (03)

Se crean 3 host que representan el sistema operativo de cada una de las 3 máquinas virtuales

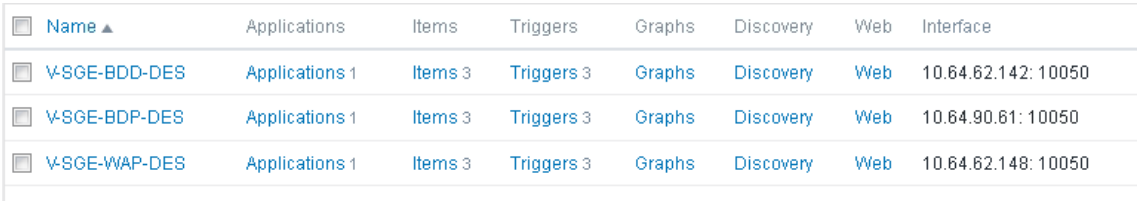


Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface
O-SGE-W1P-DES	Applications 1	Items 1	Triggers 1	Graphs	Discovery	Web	10.64.90.61: 10050
O-SGE-W2P-DES	Applications 1	Items 1	Triggers 1	Graphs	Discovery	Web	10.64.62.142: 10050
O-SGE-WAP-DES	Applications 1	Items 1	Triggers 1	Graphs	Discovery	Web	10.64.62.148: 10050

Para determinar el correcto funcionamiento del sistema operativo, se monitorea el servicio del sistema “EventSystem”

Capa MV (04)

Se crean los hosts que se corresponden con las máquinas virtuales que ejecutan los servicios necesarios para el funcionamiento de SIGED

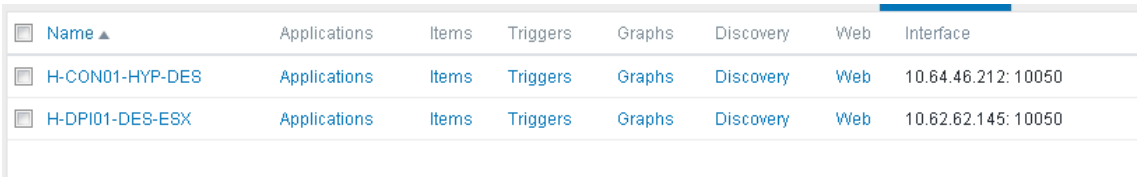


Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface
V-SGE-BDD-DES	Applications 1	Items 3	Triggers 3	Graphs	Discovery	Web	10.64.62.142: 10050
V-SGE-BDP-DES	Applications 1	Items 3	Triggers 3	Graphs	Discovery	Web	10.64.90.61: 10050
V-SGE-WAP-DES	Applications 1	Items 3	Triggers 3	Graphs	Discovery	Web	10.64.62.148: 10050

Los ítems a monitorear son ICMP Ping

Capa Hypervisor (05)

Se crean los Host que representan las instancias de HyperV y ESXi



Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface
H-CON01-HYP-DES	Applications	Items	Triggers	Graphs	Discovery	Web	10.64.46.212: 10050
H-DPI01-DES-ESX	Applications	Items	Triggers	Graphs	Discovery	Web	10.62.62.145: 10050

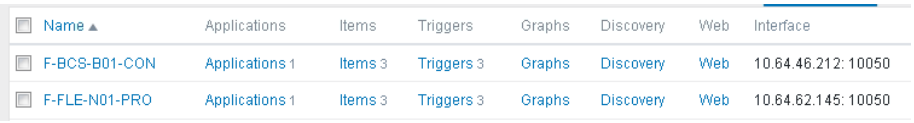
Los ítems a monitorear son los servicios que se corresponden con los hypervisores.

Capa Anfitrión (06)

Esta capa corresponde al monitoreo del NOS que cumple la función de anfitrión del Hypervisor, en el caso de implementar el modelo “No Nativo” de virtualización. Por lo cual se sigue la misma configuración para su monitoreo empleado en la Capa Operativo (3).

Capa física (07)

Se crean los Host que se corresponden con los servidores físicos.



Name ▲	Applications	Items	Triggers	Graphs	Discovery	Web	Interface
F-BCS-B01-CON	Applications 1	Items 3	Triggers 3	Graphs	Discovery	Web	10.64.46.212: 10050
F-FLE-N01-PRO	Applications 1	Items 3	Triggers 3	Graphs	Discovery	Web	10.64.62.145: 10050

A cada uno se le agrega el ítem ICMP Ping para monitorear

Capa Conectividad (08)

Esta capa, en la primera etapa del proyecto no se ha configurado para el monitoreo. Si bien es fundamental para el proceso de monitoreo, al estar administrada y gestionada por una unidad independiente como esa la Dir. de Conectividad y Telecomunicaciones, se decidió incluirla más adelante, en la etapa siguiente de configuración de la herramienta Zabbix.

Gestión de Documento

A. Historial de Cambios

Fecha	Versión	Autor	Detalle
01Dic17	1.0	Horacio SANCHEZ	Creación.

B. Revisión

Revisión	Rol

C. Aprobación

Aprobación	Rol

Autores

- Lic. Daniel J. GALLARDO
- Mag. Lic. Horacio D. SANCHEZ

Consultores Externos – Consejo Federal de Inversiones

Estabilización de la Infraestructura TI

Ahora bien, el Modelo de Monitoreo que se propone, representa un base sobre la cual comenzar a iniciar el camino de estabilización de la Infraestructura de Tecnologías de la Información (ITI). El modelo presenta una base teórica sobre la cual comenzar a identificar, especificar y documentar cada uno de los componentes que conforman la ITI asociada.

En la medida que se vaya aplicando el modelo, es necesario comenzar a definir los procesos correspondientes a la operación y administración de la Infraestructura. Para que estos procesos, y procedimientos puedan gestionarse, es fundamental comenzar a definir roles y áreas. Como así también la asignación de responsabilidades. El ordenamiento de los RRHHs es fundamental en esta etapa. Lo anterior es básico, y muy necesario. Es aconsejable que las responsabilidades estén bien determinadas, y en especial conocidas por todos los participantes de la organización. Así surge la necesidad de que una vez que estén definidos, se comiencen a gestionar los roles y las áreas.

Gestión de Roles y Áreas

El modelo define claramente una división, clasificación e identificación de los componentes en cada una de las capas. En base a esta división, es posible llevar a cabo la definición de responsabilidades y la creación de los roles correspondientes. Esto surge naturalmente, a raíz de la naturaleza inherente de la metodología de estratificación optada para modelar. Así, por ejemplo, la Capa 3 (Operativos) que corresponde a los Sistemas Operativos, englobará todas las instalaciones de NOS de servidores. A partir de lo anterior, podemos crear un rol que sea la gestión de los NOSs. Este rol, tendrá la responsabilidad de administrar y mantener en operación cada uno de los Sistemas Operativos. Así, ante un incidente registrado en alguno de los componentes pertenecientes a esa capa, será responsabilidad de los agentes que tengan asignado ese rol. Es decir, se comienza a dividir y definir responsabilidades. Se pueden modelar y especificar las tareas y procesos involucrados en la gestión de esa Capa. Y una vez modelados, y definidos quienes

los consumirían, se comienza a definir el ciclo de vida de la operación de la ITI asociada a esta capa.

Podemos analizar, según lo plateado, cada una de las capas; y así ir definiendo responsabilidades y creando los roles específicos. Es importante entender que se están definiendo roles, y no puestos de trabajo. Por lo cual, a cierto grupo de trabajo se le pueden asignar varios roles. Complementariamente, es posible subdividir los conjuntos de componentes en sub grupos, a fin de facilitar la gestión y controlar la complejidad subyacente. Esta subdivisión se puede entender en función de los ámbitos que se vayan definiendo. De esta manera, la estratificación presenta una división de los componentes a nivel vertical, y la definición de ámbitos los hace a nivel horizontal.

Sin duda alguna que lo hasta aquí planteado puede sentar las bases del inicio de la estabilización de la administración y gestión de la ITI, lo cual es algo altamente conveniente para toda organización.

Operación del SGR Zabbix

En el proceso de madurez del ciclo de vida de la operación de la Infraestructura TI, se debe avanzar en forma ordenada y siguiendo alguno de los estándares ya establecidos. Sin embargo, debido al estadío inicial de madurez en el que se encuentra el área de Infraestructura TI del a SGP, sería aconsejable iniciar la implementación de determinadas acciones. Acciones que permitan comenzar a elevar el nivel de madurez, o quizás comenzar a estabilizar el Nivel 1.

Complementariamente a la definición de componentes de la ITI que se vaya decidiendo monitorear, es necesario comenzar a definir los procesos inherentes a la operación del monitor propiamente dicho. Un punto central es definir el grupo de agentes encargados de operar el Sistema de Gestión de Red. Este grupo de agentes, los cuales tendrán asignado el rol de operación del monitor, deberían ser los destinatarios primarios de las alertas y avisos que emita el SGR (por cualquiera de las vías definidas). Este grupo conformaría el primer nivel de monitoreo. Serán los responsables de estar atentos a los incidentes que ocurran y que sean reportados. Complementariamente deberían poseer el conocimiento global de la infraestructura

monitoreada, a fin de poder determinar el impacto en la misma, de cada uno de los incidentes que se presenten. Así, ante un incidente, el monitor reportaría a este grupo de primer nivel. Este grupo, debería poder identificar y clasificar el nivel de impacto del incidente en la infraestructura. Y posteriormente, realizar los pasos necesarios para concretar la derivación hacia el área técnica especifica responsable de la solución. Esta área técnica, representaría el segundo nivel de soporte. Lo descripto, sería un primer paso simple de implementar y muy importante.

Integración de Herramientas de Gestión de Infraestructura TI

Como ya se comentó en el presente informe, es necesario a partir de la implementación del SGR, comenzar a trabajar en el modelado de procesos asociados. Todo incidente que se genere, previamente configurado en el monitor, debe ser modelado detalladamente. Así, al detectarse que cierto cambio de estado en la infraestructura es considerado como un incidente, el SGR lo detecta, lo registra, lo informa, y termina su acción.

Ahora bien, lo enunciado en el párrafo anterior, presenta la posibilidad de iniciar un proceso de mayor alcance. Es decir, no solo detectar e informar los incidentes, sino complementariamente iniciar la resolución del mismo.

Existen numerosas aplicaciones de Administración de Mesas de Ayuda en el mercado. De hecho, en el ámbito del Gobierno Provincial existen dos implementaciones operativas en distinto nivel de madurez. Dentro de la SGP, se ha implementado “Redmine” y en la Dir. de Conectividad y Telecomunicaciones se viene realizando el seguimiento y gestión de tickets de mesa de ayuda empleando “GLPI”.

De lo expresado, surge naturalmente la posibilidad ante la existencia de un incidente en la Infraestructura, que el mismo sea detectado por el SGR, informado, y posteriormente genere el ticket correspondiente en el sistema de Administración de Mesa de Ayuda. Acto seguido, automáticamente se da inicio el proceso de resolución asociado. No es necesaria la intervención humana para la generación del ticket. La vinculación entre los dos sistemas que participan se realiza a través de las APIs correspondientes. Pero es necesario llevar a cabo esta integración.

Como resumen de lo expuesto, queda claro que la potencialidad de poder integrar las distintas herramientas de gestión de Infraestructura TI es altamente beneficioso para toda la Organización. Pero, es fundamental comprender la necesidad de llevar adelante un proyecto de modelado de todos los procesos involucrados. Sin los procesos debidamente identificados, modelados y documentados; la integración y la gestión de incidentes se torna caótica y compleja.

Desde esta consultoría se propone iniciar el camino hacia la integración mencionada. E iniciar el análisis para la integración de otras herramientas complementarias.

ANEXOS

A continuación, se detalla el listado de los formularios que se relevaron y se adjuntan como anexos al presente informe.

N°	Nombre del Archivo
1	F100 - COMPROMISO DE CONFIDENCIALIDAD.docx
2	F101 - SOLICITUD DE USUARIO SIIF v6.2.doc
3	F101B - Descripción Tareas Habilitado para SIIF v1.docx
4	F103 - SOLICITUD CAMBIO DE CONTRASEÑA SISTEMAS v6.docx
5	F104 - SOLICITUD DE CONTRASEÑA PARA IMPLEMENTADOR.docx
6	F105 - SOLICITUD DE USUARIO DE EMERGENCIA.docx
7	F106 - COMUNICACION DE USUARIO Y CLAVE.docx
8	F107 - CONTINGENCIA - FORM PARA USUARIOS (Prueba Controlada).docx
9	F109 - SOLICITUD DE REQUERIMIENTO DE INFORME v4 (Abril 2015).docx
10	F111 - SOLICITUD DE USUARIO SI v6.2.doc
11	F112 - SOLICITUD DE USUARIO SIGOP v6.2.doc
12	F113 - SOLICITUD DE USUARIO IPV v6.2.doc
13	F114 - SOLICITUD DE USUARIO SIGED v6.2.doc
14	F115 - SOLICITUD DE USUARIO SIARH v6.2.doc
15	Formulario Correo v4.pdf
16	F101E - Formulario_de_Acceso_a_Sistemas_Integrados.pdf

Tabla 11 – Listado de Formularios Adjuntos al Informe