UNIVERSIDAD NACIONAL DE LA MATANZA

Escuela de Posgrado

Tesis de Maestría en Informática

"Análisis, diseño y bases de despliegue de un Servicio de Directorio, basado en una Arquitectura de Referencia, aplicable a pequeñas y medianas organizaciones".

Autor: ***Lic. Horacio D. SANCHEZ***

Director: ***Mg. Jorge ETEROVIC***

Buenos Aires, Diciembre 2014

Dedicatoria

Este trabajo quisiera dedicárselo a mi querida esposa Daniela, quien con su amor, y compañía vuelve tan lindo nuestro camino.

A mis tres queridísimos hijos Agustina, Nicolás y Malena; quienes todo el tiempo nos enseñan las cosas lindas de la vida.

A toda esa familia cercana que constituye el círculo de contención, que todos queremos y necesitamos para disfrutar lo que hacemos.

..... y un recuerdo único y especial para mis viejos, los cuales están siempre presentes.

Contenidos

Resumen

En la actualidad la infraestructura involucrada en las Tecnologías de la Información es un activo estratégico. Complementariamente, constituye el cimiento crítico sobre el cual el software y sistemas pueden ofrecer los servicios que cualquier organización moderna necesita para desarrollarse y operar de manera efectiva. Lo anterior es algo conocido, ¿Pero es realmente comprendido?

Entender, para luego modelar cada uno de los problemas y realidades asociados a la gestión de la información de la TI es altamente deseable. Dimensionar las organizaciones para enfocar los esfuerzos, teniendo en cuenta sus necesidades y requerimientos, es algo básico y fundamental. Existen determinadas claves que contribuyen a potenciar fuertemente la subsistencia y el desarrollo de las organizaciones, en especial frente al avance tecnológico y la creciente complejidad. El presente estudio se orienta a las Organizaciones Medianas, las cuales poseen determinadas características que las hacen únicas. Conceptos esenciales como simplificar, integrar, reutilizar y aplicar estándares; entre otros son básicos para gestionar tecnología en forma óptima.

Uno de los principales componentes de infraestructura tecnológica que conforman la base a nivel de infraestructura de servicios TI, es sin duda alguna el Servicio de Directorio (en adelante SD). Este servicio se vincula transversal y directamente con los restantes componentes tecnológicos y sistemas, definiéndose como la unidad básica aglutinadora. Permite que los elementos de información se correlacionen, se administren y se distribuyan manteniendo una coherencia y correcta relación entre los mismos. Además facilita la administración y gestión de la seguridad de la infraestructura TI en forma simple y centralizada.

Las organizaciones deben considerar seriamente la necesidad de adoptar estándares; evolucionar hacia estos, los que le permitirán alcanzar una deseable capacidad de adaptación. Variables como la complejidad, el cambio, la innovación, costos sustanciales y demás, asociados a la rápida transformación de los ambientes tecnológicos representan un desafío a ser considerado muy seriamente. La eficacia significativa se presenta del hecho de no tener que reinventar la rueda y resolver reiteradamente los mismos problemas. Adoptar soluciones ya probadas y exitosas, se torna muy interesante y hasta vital. Esto nos permite ahorrar tiempo valioso y a la vez escaso, para emplearlo en alcanzar los objetivos organizacionales. La propuesta de

tender hacia entornos operativos (o “ecosistemas”), en lugar de ir hacia productos tecnológicos se presenta como una directriz. Es aconsejable ver las soluciones desde una visión global e integradora. Mirar más allá del corto plazo.

De esta forma implementar un Servicio de Directorio en una organización mediana bajo la aplicación de estándares empleando guías de diseño, guías de despliegue y de operación es algo deseable y necesario. Así, en el presente trabajo se presenta el análisis, diseño y bases de despliegue de un Servicio de Directorio, basado en una Arquitectura de Referencia, aplicable a Pequeñas y Medianas Organizaciones.

CAPITULO I: PLANTEO DE LA PROBLEMÁTICA

DESCRIPCION GENERAL DEL PROBLEMA

En las organizaciones modernas la infraestructura involucrada en las Tecnologías de la Información (TI en adelante) es un activo estratégico. Y representa el cimiento crítico sobre el cual software y aplicaciones pueden ofrecer los servicios que necesita cualquier organización para operar de manera efectiva y desarrollarse. Lo anterior es algo conocido, ¿Pero es comprendido realmente?

Para muchas organizaciones la evolución natural y el vertiginoso desarrollo de las nuevas tecnologías, en el tiempo, ha producido como resultado infraestructura tecnológica demasiado compleja. Como así también inflexible y difícil de administrar. Con costos integrados que además de ser altos, de alguna manera son fijos y sin mantener una relación con los requisitos u objetivos de la organización.

La mayoría de las organizaciones reconocen la importancia de una infraestructura de TI optimizada y eficaz. Por lo descripto se intenta racionalizarla e incrementar su eficiencia operativa a través de iniciativas tales como la consolidación del centro de datos, la estandarización de escritorios de trabajo o entornos operativos, la implementación de mejores prácticas operativas en lo referente a TI, entre otras. Tales iniciativas desarrolladas por las áreas de TI de manera aislada, o focalizadas aisladamente en determinadas áreas, no serán suficientes por sí mismas para brindar a largo plazo las mejoras deseadas que son demandadas.

Es común también la necesidad de manejar adecuadamente las diversas clases de información que crean y utilizan a diario las organizaciones. De importancia particular para este estudio, es la información referente a la organización de la infraestructura TI en sí misma, tal como lo son nombres y apellidos de personas, códigos de usuarios y recursos computacionales, direccionamientos de los tipos más diversos, asignación y gestión de claves o certificados de seguridad, derechos de acceso a diferentes recursos, por citar algunos ejemplos. Es deseable que estos elementos de información se correlacionen, se administren y se distribuyan manteniendo una correcta relación entre los mismos. Sin embargo, esto último no es común que suceda. Es frecuente encontrar el mismo ítem de dato en diversas formas, o credenciales de seguridad de los usuarios de los diversos sistemas almacenados en una localización, y los roles de estos mismos usuarios almacenados y manejados en otra distinta. Lo descripto involucra el histórico problema de las ABM (Altas, Bajas y

Modificaciones). Con el agravante que estamos sumando una dimensión adicional, de una gran importancia, como es la seguridad.

La tarea de conciliar un escenario de cambios y administrar la información citada en una forma coherente se torna vital, mientras que el soporte de su distribución y rápida recuperación se convierte cada vez en algo más importante y a la vez más complejo. Esta información se emplea como apoyo directo a la administración y gestión de los recursos de usuarios y de componentes de cómputos. Esto determina que la eficiencia con la cual se maneja tiene un impacto directo en la organización y en la complejidad asociada. Como ejemplo podemos citar sistemas de información que administran información de usuarios, autentificación y mecanismos del control de acceso que se solapan con los de los sistemas operativos de red o sistemas de mensajería; generando un aumento perceptible del costo de administrar el ambiente. Lo anterior involucra, quizás, que un mayor número de personal sea necesario para gestionar los servicios adicionales de autentificación y validación. Así también comienza a crecer en forma conjunta la posibilidad de fallas e inconsistencias debido a cuestiones de interoperabilidad. Además, la seguridad se debilita inevitablemente producto de la complejidad en el manejo de los derechos y permisos al interactuar con los modernos ambientes heterogéneos de trabajo. Así surgen un gran número de configuraciones potencialmente válidas, pero solo unas cuantas resultan integradas en un sistema funcional. La determinación de las configuraciones correctas, la implementación y mantenimiento puede resultar en una solución con costos y complejidad asociados muy elevados.

Lo anterior afecta a todas las organizaciones y a la organización en su conjunto, esencialmente es una problemática transversal a la misma. Todos los departamentos o unidades, seguramente interactuarán o requerirán servicios basados en información referida a usuarios y recursos computacionales. Este tipo de problemática trasciende los límites del área de TI. Los servicios y la información de este tipo son requeridos por usuarios internos y externos, alumnos, docentes, aplicaciones en todos sus tipos y niveles, proveedores, socios de negocio, colaboradores externos, auditores, entre otros. (Microsoft, 2007)

Por razones culturales profundas, nuestras organizaciones suelen adolecer de la planificación a mediano y largo plazo. En particular a la que se refiere este trabajo, es la planificación del desarrollo del crecimiento en infraestructura de servicios de TI. Las

organizaciones crecen sin esta planificación, y esto impacta fuertemente en diversas dimensiones, especialmente en lo referido a complejidad y costos.

Las Pequeñas y Medianas Organizaciones (en adelante PyMO, Ver definición más adelante en página 59), frecuentemente no poseen los recursos para ensayar de una forma adecuada las configuraciones de sus sistemas de TI y asegurar que sean funcionales a sus requerimientos. Producto de lo anterior, les es difícil aseverar que los distintos sistemas sean estables y confiables. Al paso del tiempo, los sistemas pueden tender hacia la inestabilidad y perder su confiabilidad. Así, las modificaciones naturales propias de la evolución de los mismos frecuentemente son realizadas bajo presión para hacer frente a cambios o resolver lo relacionado a los servicios. Esto naturalmente conduce a que la tecnología subyacente se convierta en algo desconocido. Gradualmente, el costo de correr y cambiar el sistema de acuerdo con los requerimientos de los objetivos organizacionales tiende a salirse de control, incrementando su complejidad y restando confiabilidad.

El avance tecnológico natural de cada uno de los componentes de la Infraestructura de TI involucra la necesidad de centralizar e integrar lo referente a la información y servicios de TI. Desde un punto de vista lógico, en organizaciones grandes este concepto de centralización incorpora una mezcla compleja de productos de diversos vendedores de hardware y software como también se hace necesario contar con numerosos profesionales especializados en tecnología. Este conjunto de recursos provee servicios a todo lo largo del denominado “Ciclo de Vida de la TI”. Realizando una analogía con la realidad de una PyMO cuyo volumen organizacional será menor, seguramente en lo referente a complejidad tendrá un impacto proporcionalmente mayor. Es decir, los niveles de complejidad no disminuyen directamente en relación al tamaño de la organización. Hay conceptos básicos de aplicación de tecnología que se deben cumplir y estos acarrean niveles considerables de complejidad. Lo anterior se entiende un poco mejor, si relacionamos la cantidad de profesionales en TI que poseen las organizaciones medianas y pequeñas y los niveles de servicios que deben asegurar. Los servicios se descomponen en unidades menores, las cuales idealmente deben ser integradas para asegurar que funcionen correctamente. El rango de estas unidades en la actualidad es elevado.

Las PyMOs poseen personal limitado, con habilidades limitadas, en especial en las áreas de TI. Vamos a definirlos como “Informáticos Generalistas”. Este personal no es especialistas en ninguna tecnología en particular, pero deben poseer el

conocimiento en una gran variedad de las mismas. Ellos son los responsables de proveer servicios a lo largo del ciclo de vida de TI. Esta es una de las características particulares de este tipo de organización, y uno de los limitantes para su crecimiento. Con el paso del tiempo, y sumado a las características específicas de las soluciones que se van adoptando e implementando (mixtura tecnológica), estos profesionales son difíciles de ser reemplazados. Y, una nueva incorporación, conlleva un largo período de formación asociado.

Otro objetivo básico actual, es el de elevar los niveles de interoperabilidad entre los distintos sistemas que se encuentran dentro de las Organizaciones. La interoperabilidad tiene como uno de sus pilares, la necesidad de contar con repositorios comunes de cierto tipo de información. Si analizamos y relacionamos lo antes presentado coincidiremos que estamos hablando de conceptos significativamente parecidos.

JUSTIFICACION

En relación a la implementación de soluciones de TI, cada organización posee requerimientos únicos. Estos requerimientos conforman o constituyen parte de lo que define la identidad organizacional. Al momento de implementar cualquier tipo de solución, seguramente será necesario involucrar trabajo adicional para satisfacer estos requerimientos. Algunas veces, en base a la perspectiva de años y con una dirección paso a paso será posible satisfacerlos. Todo procedimiento o solución en servicios TI al ser diseñados se desarrollan con la premisa que luego de ser adoptados, requerirán futuras adecuaciones para alcanzar los requisitos particulares de la organización y la evolución de la tecnología subyacente. En base a lo anterior, contar con una guía o conjunto de opciones de diseño deseablemente cercanas a las mejores prácticas, y adaptables a la cultura organizacional sería algo muy bueno. Estas guías deberían poder ser usadas para implementar una solución específica o un conjunto de ellas. Y entender que decisiones de entre las disponibles son factibles, y porque una decisión debe ser tomada en un escenario determinado y como desplegarla. Sería interesante también, contar con documentación que ofrezca información de integración de tecnología que ya haya sido probada para resolver metas arquitectónicas específicas como lo son la disponibilidad, seguridad, escalabilidad, manejabilidad, por nombrar algunas de entre las principales.

Las claves que ayudan fuertemente a la subsistencia en el medio actual de las PyMOs son entre otras las de lograr simplificar, integrar, reusar y aplicar estándares. Y estas claves son las constantes a mantener para afianzar el crecimiento. Considerando lo enunciado en el párrafo anterior, uno de los componentes que conforman la base tecnológica a nivel de sistemas de infraestructura de servicios TI es sin duda alguna el Servicio de Directorio. Más adelante veremos una definición bien detallada de lo que es y que involucra este servicio. El SD se vincula transversal y directamente con los restantes componentes, y cada vez más se afianza como la unidad básica aglutinadora de los restantes servicios. Así, permite que los elementos de información se correlacionen, se administren y se distribuyan manteniendo una coherencia y correcta relación entre los mismos.

Como complemento, desde el momento que se administra información de recursos TI, surge la necesidad de contar con un método de almacenarla en forma segura, controlando la replicación, su sincronización y distribución. La tecnología a adoptar debe poder escalar tanto horizontal como verticalmente, como así también

soportar fragmentación en ambas dimensiones. Es necesario poder recuperar la información almacenada mediante métodos estándares de acceso en base a diversos criterios. Esta estandarización debe abarcar numerosos ambientes operativos de trabajo.

La estructura del repositorio de información, lo que en los SD se denomina “esquema”, es deseable que sea suficientemente dinámica para acompañar los continuos cambios en los requerimientos. Esto facilitará el almacenamiento de diversos tipos de información, sin mayores repercusiones. A lo anterior, algunos autores lo citan como la propiedad de “extensibilidad” del esquema del directorio. (HOWES, GOOD, & SMITH, 2003).

Una vez almacenada la información, sería necesario poder ejercer control sobre la seguridad de la misma. Se tornaría imprescindible acceder a los datos en función de diferentes criterios de seguridad, pudiendo configurar la granularidad, su modularidad y aplicar un concepto relativamente nuevo en lo que a implementación se refiere, que es la “versatilidad de la delegación de administración”.

Contar con soporte a la distribución de los certificados electrónicos personales es esencial. Y es fundamental resolver estos dos problemas bases: primero la gestión de la infraestructura de clave pública, y segundo el problema de la ubicación de los certificados.

Analizando lo expuesto, es posible deducir que un servicio con estas características es importante en sí mismo. Pero entendamos la potencialidad que adquiere si puede ser el elemento aglutinador y una de las herramientas faltantes para desarrollar aplicaciones que permitan desplegar nuevos servicios basados en la cooperación de las mismas y este servicio. Tengamos en cuenta que hablamos del Servicio de Directorio.

Del análisis de lo anterior surge la necesidad de llevar a cabo un estudio profundo de este servicio, desde sus aspectos técnicos, como así también desde un punto de vista vital del desarrollo y proyección de las TICs dentro de las organizaciones.

Si analizamos algo básico en relación a lo estratégico en lo que a Gestión de TI se refiere, es muy común que aparezca el presentimiento que se está analizando y/o diseñando algo que ya se ha hecho antes. Lo anterior en relación al despliegue y diseño de TI. ¿Cuántas veces, todavía, las ruedas siguen reinventándose?, ¿Que costos asociados tiene reinventar? Y como algo alternativo ¿Qué beneficios aporta el

adecuar o copiar? Al ensayar las respuestas a estos cuestionamientos, surge naturalmente la necesidad de considerar una “Arquitectura de Referencia” (AR en adelante). Una AR es la especificación de infraestructura estandarizada y pre-comprobada. Un conjunto de soluciones o guías listas para implementarse para distintos escenarios tecnológicos comparables. Lo anterior permite que quien lleve a delante un proyecto de TI basándose en una AR, se centre principalmente en los aspectos únicos y diferenciales su proyecto. Así, se dejan de lado los aspectos repetitivos y genéricos naturales de un despliegue tecnológico.

Así, incorporar una AR puede involucrar:

• Una guía que oriente eficazmente. Es decir, un factor decisivo para una organización que desarrolla un entorno de operaciones estándar en el que deberían poder incluirse diversas soluciones e infraestructuras.

• Entornos probados e integración. Posibilidad de trabajar sobre escenarios típicos, ya probados en laboratorio, y que en numerosas ocasiones facilita la cooperación con posibles asociados. Lo anterior contribuye notablemente al desempeño de niveles de servicio deseables.

• Factibilidad de controlar costos e identificarlos con un rendimiento predecible y confiable. Las configuraciones probadas en laboratorio son más confiables y más rápidas de implementar. Poseen un Costo Total de Propiedad (TCO, según su siglas en inglés) más bajo. Es posible contar con una lista de materiales predeterminada, criterios de medición del rendimiento adecuado y pautas para la implementación que reducen considerablemente los costos de la implementación.

• Flexibilidad a la hora de implementar e integrar. Se simplifica sensiblemente la integración con entornos y estándares existentes, la decisión de seleccionar productos, configuraciones y posibilidades existentes en la industria.

• Integración. Las configuraciones basadas en una AR normalmente incluyen los procesos y las funciones organizacionales básicas para comenzar a utilizar los componentes de la arquitectura inmediatamente.

• Tecnologías probadas. Las configuraciones que se emplean de guía, normalmente se basan en las tecnologías reconocidas. Estas tecnologías han sido diseñadas creadas y probadas en ambientes de laboratorio.

La siguiente figura representa las ventajas en cuanto al tiempo de implementación de componentes tecnológicos al basarse en una AR respecto a hacerlo en la forma tradicional implementando cada componente en forma aislada. El sector anaranjado representa el trabajo basado en una AR, el trabajo repetitivo, conocido, estudiado y modelado. El verde, lo particular y distintivo del proyecto.

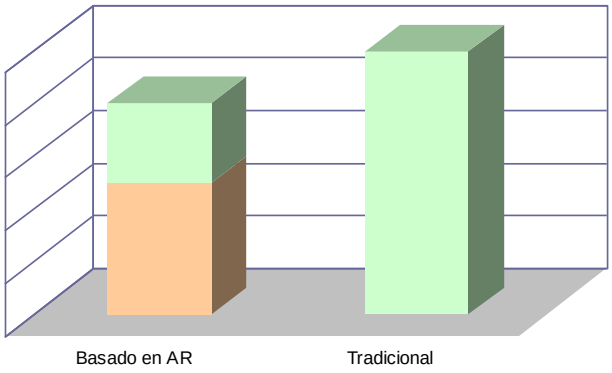

Ilustración 1. Ventajas de basarse en una Arquitectura de Referencia.

En organizaciones medianas la planificación de la próxima generación de infraestructura técnica para ellas puede ser una tarea compleja y de enormes proporciones. Si se hace bien, las capacidades de la Tecnología de la Información (TI) estará bien alineada con “los objetivos organizacionales” y se convertirá en un activo estratégico. Si se hace mal, puede ser un obstáculo difícil de superar. Lo anterior debe analizarse bajo la premisa de la limitación en lo referido a recursos con que se cuenta a este nivel.

El éxito de toda la infraestructura se mide en lo bien que las decisiones tomadas en relación con la infraestructura coinciden con los objetivos de la Organización. Aunque a menudo hay cientos o incluso miles de páginas de documentación de los productos existentes, históricamente ha sido muy difícil encontrar una guía sobre cómo planificar adecuadamente la infraestructura básica para una organización. (Solutions Accelerators, 2009). Una arquitectura de referencia provee a las organizaciones una base para la estandarización, incorporando las mejores prácticas y ayudando a la implementación inicial de los proyectos. La eficacia significativa se presenta del hecho de no tener que reinventar la rueda y resolver reiteradamente los mismos problemas entre otros. (Microsoft, 2003).

Presentado lo anterior, surge la necesidad de efectuar un análisis integrado y de mayor profundidad respecto de los dos ejes centrales. Veamos, uno de ellos es el Servicio de Directorio. El segundo, lo asociado al empleo de una Arquitectura de Referencia en el despliegue de un SD. Así la necesidad casi imperiosa en una organización moderna de contar con una implementación de un Servicio de Directorio y la adopción de una metodología de diseño, despliegue y operación basada en una AR, se transforma en un proyecto directriz.

ALCANCE

La presente tesis se enfocará en el proceso de diseño de un Servicio de Directorio de red en el entorno de una Organización Mediana o Pequeña, basándose en una arquitectura de referencia. Se completarán especificación de procesos y guías básicas de análisis. Lo anterior permitirá comprender, por parte de los especialistas en Tecnologías de la Información de las organizaciones, el proceso de diseño en todas sus fases, sirviendo de base para la toma de decisiones.

El propósito de este trabajo es ayudar a los diseñadores de arquitecturas de TI en la toma de decisiones, proporcionando un camino claro y conciso para el diseño de la infraestructura de un Servicio de Directorio, en un contexto relativo. Este trabajo se basa en las mejores prácticas y experiencia del mundo real para ofrecer consideraciones y alternativas en cada punto del diseño.

OBJETIVO GENERAL

El objetivo general de esta tesis es generar un documento guía que permita a los informáticos generalistas de las PyMOs comprender el alcance y diseñar un Servicio de Directorio aplicable en Organizaciones Pequeñas y Medianas.

OBJETIVOS ESPECIFICOS

- Definir que es una organización mediana y pequeña.
- Definir el flujo de decisiones técnicas a través del proceso de diseño de un Servicio de Directorio.
- Describir los considerandos a tener en cuenta y las opciones disponibles a considerar en la toma de decisiones en el proceso de diseño.
- Relacionar las decisiones y las opciones con los objetivos organizacionales en términos de costos, complejidad, y otras características relevantes.
- Describir el marco tecnológico subyacente necesario para el desarrollo de un Servicio de Directorio en una PyMO.
- Enmarcar las decisiones en términos de preguntas adicionales a los Informáticos Generalistas a fin de consolidar una comprensión completa del panorama de objetivos organizacionales adecuados.

CAPITULO II: BASES TEORICAS

ANTECEDENTES Y MARCO TEÓRICO

Servicio de Directorio

Historia del Servicio de Directorio – X.500

En 1984, la ITU-T (por entonces llamada CCITT) decidió desarrollar especificaciones de un directorio de propósito general. La necesidad más inmediata fue proporcionar un directorio para el tratamiento de mensajes (X.400). La ISO/IEC JTC1 había iniciado una actividad similar. Ambas organizaciones acordaron entonces en fusionar las dos actividades en una única actividad de colaboración con el fin de evitar la generación de dos normas diferentes para el mismo propósito. Esta colaboración fue muy productiva y se la denominó “Directorio OSI”, y sobre la cual se trabaja hasta la actualidad (x500 Standard, 2001).

Como resultado de ese trabajo conjunto entre la ISO/IEC y la ITU-T se ha publicado estándares prácticamente idénticos que sólo difieren en el prólogo de apertura de los documentos. Se ha presentado como el estándar Internacional ISO/IEC 9594 y como la serie de recomendaciones X.500 de la ITU-T. Una tabla con los identificadores correspondientes de la ISO y la ITU-T se muestra a continuación.

Titulo Completo	Recomendación	Estándar
Information technology – Open Systems Interconnection – The Directory: Overview of Concepts, Models, and Services	ITU-T Rec. X.500	ISO/IEC 9594-1
Information technology – Open Systems Interconnection – The Directory: Models	ITU-T Rec. X.501	ISO/IEC 9594-2
Information technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks	ITU-T Rec. X.509	ISO/IEC 9594-8
Information technology – Open Systems Interconnection – The Directory: Abstract Service Definition	ITU-T Rec. X.511	ISO/IEC 9594-3
Information technology – Open Systems Interconnection – The Directory: Procedures for Distributed Operation	ITU-T Rec. X.518	ISO/IEC 9594-4
Information technology – Open Systems Interconnection – The Directory: Protocol Specifications	ITU-T Rec. X.519	ISO/IEC 9594-5
Information technology – Open Systems Interconnection – The Directory: Selected Attribute Types	ITU-T Rec. X.520	ISO/IEC 9594-6
Information technology – Open Systems Interconnection – The Directory: Selected Object Classes	ITU-T Rec. X.521	ISO/IEC 9594-7

Titulo Completo	Recomendación	Estándar
Information technology – Open Systems Interconnection – The Directory: Replication	ITU-T Rec. X.525	ISO/IEC 9594-9
Information technology – Open Systems Interconnection – The Directory: Use of Systems Management for Administration of the Directory	ITU-T Rec. X.530	ISO/IEC 9594-10

Tabla 1. Identificadores correspondientes de la ISO y la ITU-T.

Como “X.500” es más fácil de recordar como identificador, el público lo ha adoptado como referencia convencional para todas las partes de la Norma Internacional y las recomendaciones de la serie.

Las normas OSI tenían poca penetración en el mercado, sobre todo debido a la aceptación de la industria del TCP/IP y las especificaciones relacionadas y desarrollos en el entorno de Internet. Sin embargo, el Directorio de OSI fue ganado la aceptación general. El término X.500 y las especificaciones de directorio de X.500 se utiliza como preferencia de título oficial. Las especificaciones de Directorio X.500 están documentados de idéntica forma de texto dentro del estándar ISO/IEC 9594 y en las series de recomendaciones de la ITU-T.

Son cinco las ediciones de las especificaciones del Directorio X.500 que se han emitido hasta el momento:

1. **Primera Edición**

   Esta es la primera edición y se emite en varias partes del estándar ISO/IEC 9594:1990 y como el CCITT X.500 (1988) de la serie de recomendaciones. Esta edición especifica la guía básica de los servicios, protocolos y procedimientos necesarios para las operaciones. Se especifican los modelos de información de cómo la información se estructura y especifica algunos de los objetos comunes de información utilizable. Además, proporciona un marco común para las técnicas de autenticación general.

2. **Segunda edición**

   Esta segunda edición fue publicada como ISO/IEC 9594:1995 y como X.500 UIT-T (1993). Esta edición ha añadido algunas funciones muy útiles, como remedo de la información de la guía, control de acceso y se ha ampliado

de manera significativa el modelo de información y capacidades administrativas.

3. **Tercera edición**

Esta tercera edición se publicó como ISO/IEC 9594: 1998 y como X.500 UIT-T (1997). Ofrece varios menores y algunas extensiones importantes. Se añade una característica llamada contextos, lo que permite que la información sea distinguida según los contextos en los que se accede. Otra novedad es la disposición de la OSI de gestión del Directorio. Asimismo, ha añadido y ampliado las funciones de seguridad.

4. **Cuarta edición**

Esta cuarta edición se emite en la norma ISO/IEC 9594: 2001 y como X.500 UIT-T (2001). Esta edición ofrece varias extensiones importantes. Añade funciones de gestión de servicios, correspondiente asignación basada en las familias de las entradas y apoyo a una pila pura TCP/IP.

5. **Quinta edición**

Esta quinta edición se emite en la norma ISO/IEC 9594:2005 y como X.500 UIT-T (2005). Esta edición ofrece la máxima alineación con LDAP. Se han reducido sustancialmente las especificaciones de dependencia externa de OSI.

ISO / IEC y UIT-T pueden indicar diferentes años para la misma edición, debido a diferentes reglas. El UIT-T indica el año en el que ha sido aprobado el trabajo, y la ISO / IEC indica el año de publicación oficial.

Estructura del X.500

El directorio X.500 se compone de Agentes de Sistema de Directorio, DSAs *(*en inglés *Directory System Agent)*, que mantienen la información distribuida del directorio. Éstos constan de:

- Una base de datos propia que mantiene una parte de la información global del directorio (por eso es distribuida).
- Unos procedimientos de comunicaciones que permiten el diálogo entre los DSAs así como entre ellos y los usuarios por medio de los Agentes de Usuario de Directorio, DUAs *(Directory User Agent)*.

La relación entre estos componentes se muestra en la ilustración 2.

La información que se mantiene en el directorio está compuesta por objetos, entendiendo por éstos, entes muy diversos como cosas, animales, personas, grupos, organizaciones, países, aplicaciones OSI, por citar algunos. Esta información define la estructura que luego toma forma como el esquema del SD.

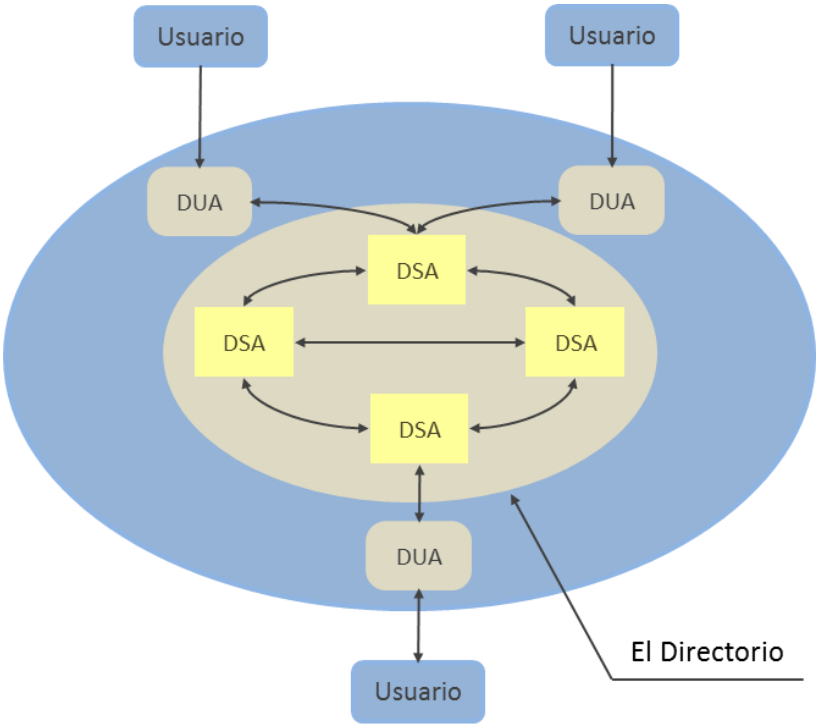

Ilustración 2. Relación entre componentes del directorio.

El concepto de entrada

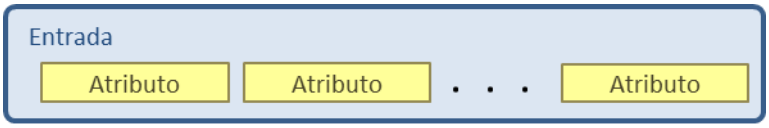

Ilustración 3. Concepto de entrada.

La información sobre un objeto, al menos conceptualmente, es almacenada en una entrada. Una representación simplificada de una entrada se muestra en la figura N° 2. La información acerca de un objeto se almacena en los atributos de la llamada. Un atributo puede ser apellido, nombre, nombre de la calle, número de teléfono, dirección de correo electrónico, certificado, contraseña, entre otros.

El protocolo LDAP fue creado como una versión liviana de X.500 y terminó por reemplazarlo. Por esta razón algunos de los conceptos y estándares que utiliza LDAP provienen de la serie de protocolos X.500.

¿Qué es un Servicio de Directorio?

Desde un punto de vista conceptual un Servicio de Directorio es una aplicación o un conjunto de sistemas que almacena y organiza la información sobre los usuarios de una red de computadoras, recursos de red, y permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red. Los SDs actúan como una capa de abstracción entre los usuarios y los recursos administrados.

Un Servicio de Directorio no debería confundirse con el repositorio de directorio, que es la base de datos que contiene la información sobre los objetos de nombrado gestionada por el Servicio de Directorio. En el caso del modelo de Servicio de Directorio distribuido en X.500 se usa uno o más espacios de nombre (árbol de objetos) para formar el Servicio de Directorio. El Servicio de Directorio proporciona la interfaz de acceso a los datos contenidos en unos o más espacios de nombre de directorio. La interfaz del SD es la encargada de gestionar la autenticación de los accesos al servicio de forma segura, actuando como autoridad central para el acceso a los recursos de sistema que manejan los datos del directorio.

Como base de datos, un servicio del directorio está altamente optimizado para lecturas y proporciona alternativas avanzadas de búsqueda en los diferentes atributos que se puedan asociar a los objetos de un directorio. Los datos que se almacenan en el directorio son definidos por un esquema extensible y modificable. Los servicios de directorio utilizan un modelo distribuido para almacenar su información y esa información generalmente está replicada entre los diversos servidores que conforman el directorio.

Un Servicio de Directorio sencillo sería, por ejemplo, un servicio de nombres para corresponder los nombres de los recursos de la red con sus respectivas direcciones de red (como ejemplo podemos citar DNS). Con este tipo de Servicio de Directorio, un usuario no tiene que recordar la dirección física de los diferentes recursos de la red, pues con saber simplemente su nombre estará accediendo al recurso demandado. Cada recurso de la red se considera como un objeto en el servidor de directorio, donde la información de un recurso en particular se almacena como atributos de ese objeto. La información que representa un objeto se establece de forma segura, accediendo a tales objetos usuarios con los permisos adecuados para poder manipular dicha

información. Directorios más sofisticados son diseñados con multitud de características y preferencias para poder manipular la información del directorio, según la dificultad de gestión que su administrador pretenda manejar.

Un servicio del directorio define el espacio de nombres de una red. Un espacio de nombres, en este contexto, es el término que se utiliza para llevar a cabo unos o más objetos como entradas nombradas. El proceso del diseño del directorio tiene normalmente un conjunto de las reglas que determinan cómo se nombran y se identifican los recursos de la red. Las reglas especifican que los nombres sean únicos e inequívocos. En X.500 (el estándar de Servicio de Directorio) y en LDAP el nombre se denomina "nombre distinguido" (DN, en inglés: D*istinguished Name*) y se utiliza para referirse al nombre único de una entrada.

Un Servicio de Directorio involucra toda la infraestructura necesaria para compartir la información para localizar, manejar, administrar, y organizar los componentes y recursos comunes de una red, que pueden incluir volúmenes, carpetas, archivos, impresoras, usuarios, grupos, dispositivos, números de teléfono, claves, certificados y otros objetos. Un SD es un componente importante del sistema operativo de red (NOS, en inglés: *Network Operating System*). En casos más complejos, un Servicio de Directorio es el repositorio central de información para una Plataforma de Entrega de Servicios. Por ejemplo, el servicio de exploración de redes conocido como servicio de *browsing* en inglés. Este servicio, al usar un Servicio de Directorio, puede entregar una lista de computadoras disponibles y la información necesaria para acceder a las mismas.

Comparación de un SD con una base de datos relacional

Es una tendencia natural la de comparar un SD con una Base de Datos Relacional. Si bien tienen similitudes importantes existe un cierto número de cosas a distinguir entre ambos.

- Dependiendo del uso del directorio, la información se lee generalmente con mayor frecuencia que con la que se escribe o modifica, por lo tanto las transacciones y las operaciones de restauración generalmente no están implementadas en algunos sistemas de directorio. Los datos suelen ser redundantes, siendo su principal objetivo las búsquedas eficientes y en especial rápidas.

- Los datos se organizan en una estructura terminantemente jerárquica que en ocasiones suele ser problemática. Para superar espacios de nombre profundos, algunos directorios desmontan la jerarquía del espacio de nombre del objeto en sus mecanismos de almacenaje para optimizar la navegación. Es decir, estos directorios buscan el ítem basándose en los atributos de los datos y después determinan sus valores del espacio de nombre, pues éste procedimiento es más rápido que la navegación de espacios de nombre grandes para buscar tal ítem. En términos de cardinalidad, los directorios tradicionales no tienen relaciones múltiples. En su lugar, tales relaciones se deben mantener explícitamente usando las listas de distintos nombres o de otros identificadores (similares a los identificadores de tabla cruzadas usados en bases de datos relacionales).

- Originalmente la jerarquía de la información de directorio del X.500 era considerada problemática contra diseños de datos relacionales. Actualmente, se desarrolla con bases de datos orientadas a objeto basadas en Java y los formularios en XML adoptan un modelo de objetos jerárquico, indicando una evolución de la ingeniería de datos relacionales tradicional.

- Un esquema se define como clases de objeto, atributos, referencias y conocimiento (espacios de nombre).

- Las clases de objeto tienen:

- Atributos-debe, cada una de las instancias que debe tener

- Atributos-puede, se puede definir para una instancia, pero podría también omitirse cuando se crea el objeto. La carencia de certeza del atributo es como un NULL en bases de datos relacionales.

- Atributos multivaluados en directorios permiten múltiples atributos de nombrado en un nivel tal como tipo de máquina y números de serie concatenados o múltiples números de teléfono para el "teléfono del trabajo".

- Los atributos y las clases de objeto se estandarizan a través de la industria y se registran formalmente en la Agencia de Asignación de Números de Internet (IANA, en inglés *Internet Assigned Numbers Authority*) para la identificación del objeto. Por lo tanto la mayoría de las implementaciones intentan reutilizar

mucha de las clases y de los atributos estándar para maximizar la ventaja de tener un Servicio de Directorio.

- Las instancias del objeto residen en los “espacios” del directorio. Es decir, cada clase de objeto hereda de su padre (y en última instancia de la raíz de la jerarquía) añadiendo atributos de la lista debe/puede.

- Los servicios de directorio son a menudo un componente central en el diseño de la seguridad de un sistema de TI, teniendo una granularidad fina con respecto al control de acceso: quién puede acceder que información y de qué manera.

El diseño del directorio es bastante diferente del diseño de una base de datos relacional. Con las bases de datos se tiende a diseñar un modelo de datos para asuntos de negocio y los requisitos de proceso, a veces on-line con el cliente, el servicio, el administrador, cuando a veces los valores de escala de presencia y sistema son omitidos. Con los directorios sin embargo, si uno está poniendo la información en un repositorio común para muchos usos y usuarios, después su diseño y esquema de la información (e identidad) debe ser desarrollado conforme a lo que está representando los objetos en la vida real. En la mayoría de los casos, estos objetos representan los usuarios, agendas, listas, preferencias, derechos, productos y servicios, dispositivos, perfiles, políticas, números de teléfono, rutas, entre otros. además uno debe también considerar los aspectos operacionales de diseño en vista del funcionamiento y de escala. Un chequeo rápido en el diseño operacional es tomar pe. 1 millón de usuarios, 50 objetos cada uno con sus usuarios o acceso a aplicaciones a estos objetos hasta 5000 por segundo, minuto, u hora (autorizar y poner al día sus servicios de entorno), y chequear si el servidor y la red considerada pueden soportar tales tareas.

La diferencia principal con las bases de datos y directorios es en el nivel de sistema donde una base de datos se utiliza para automatizar un proceso con un modelo (relacional) de datos dedicado, pero un directorio se utiliza para llevar a cabo objetos “identificados” que se pueden utilizar para muchos usos. Se aplica un Servicio de Directorio donde “está multigobernado” (muchas aplicaciones y usuarios), por razones de integridad y de eficiencia, usando la misma información. Este acercamiento al diseño del sistema da mayor escala y flexibilidad para poder especificar correctamente las funciones de una escala más grande tales como plataformas de entrega de servicios. Síntoma de ello es que las grandes compañías tienen centenares

de diseños de base de datos (si no millares) para diversos procesos y ahora están intentando converger la información de usuario y de servicio de identidad, junto a sus mercancías en línea y gestión de servicios, entrega éstos en tiempo real, coste rentable.

Desarrollos de SDs

La gran mayoría de implementaciones están basados en el estándar X.500, que posteriormente fue la base de LDAP, pero utilizando la pila TCP/IP en vez de usar el modelo OSI, adquiriendo especial relevancia en internet.

Existen numerosas formas de implementación de servicios de directorio de diferentes compañías. Algunos de estos ejemplos son:

NIS Network Information Service protocolo, nombrado originalmente como Páginas Amarillas, implementación de Sun Microsystems' en un Servicio de Directorio para redes de entorno UNIX. (Sun, a principios del 2000, se unió a iPlanet, alianza de Netscape y desarrolló la base de LDAP, Servicio de Directorio que formó parte de Sun ONE.

eDirectory, desarrollado por Novell, es un Servicio de Directorio que soporta múltiples arquitecturas incluyendo Windows, NetWare, Linux, incluyendo algunas distribuciones de Unix. Se ha utilizado durante tiempo para la administración de usuarios, gestión de configuraciones y gestión de software. eDirectory se ha desarrollado como componente central en una gama más amplia de productos para la gestión de identidad. Fue conocido previamente como servicios de directorio de Novell.

Servidor de directorio de Red Hat: Red Hat lanzó un servicio del directorio, que adquirió de Netscape Security Solutions de AOL, el cual funcionaba como producto comercial bajo Red Hat Enterprise Linux denominado como servidor de directorio de Red Hat como parte del núcleo de Fedora.

CentOS Directory Server: CentOS Directory Server está basado en Red Hat Directory Server, posee similares características, y está disponible para instalar vía Yum, sin necesidad de tener un contrato de por medio. La base del software está licenciada bajo GNU/GPL 2, y se incluye una excepción para ser integrado con software no libre, la cual proviene de RedHat.

Active Directory: El servicio del directorio de Microsoft, es el directorio que se incluye en las versiones de los sistemas operativos de Windows 2000/2003/2008 y 2012. Es reconocido como uno de los más evolucionados.

Open Directory: El servidor del Mac OS X de Apple ofrece un servicio del directorio llamado Open Directory que integra muchos protocolos estándares abiertos tales como LDAP y Kerberos así como soluciones propietarias de directorio como Active Directory y eDirectory.

Servidor de directorio de Apache: Apache Software Fundation ofrece un servicio del directorio llamado ApacheDS.

Directorio de Internet de Oracle: (OID) es el servicio del directorio de Oracle Corporation, que es compatible con la versión 3 de LDAP.

Directorio CA: El directorio CA contiene un motor de caché previo que puede indexar todos los atributos que se usan en los filtros de búsqueda de LDAP, y poner en cache aquellos atributos devueltos en tales búsquedas. Teniendo bastante memoria, el directorio CA es el directorio más rápido del planeta.

OpenDS: La nueva generación de Servicio de Directorio abierto ofrecido por Sun Microsystems.

Hay también numerosas herramientas de código abierto para implementar servicios de directorio, incluyendo OpenLDAP, protocolo Kerberos o el software de Samba, el cual puede actuar como controlador de dominio con Kerberos y estar implementado con LDAP.

Nueva Generación de sistemas de directorio

Las bases de datos junto a la industria de las TI han permanecido ligadas desde la era del ordenador hasta los directorios tradicionales, pasando entre 20-30 años, y estarán con nosotros en el futuro. Sin embargo, con una escala superior, los servicios convergentes y los sistemas conducidos por la presencia (por ejemplo IMS sobre 3G), requerirán una cierta evolución. Esto podría tomar la forma de Servicio de Directorio Adaptado Compuesto (CADS, en inglés *Composite Adaptive Directory Services*). CADS es un servicio avanzado de directorio y contiene funciones para la gestión de identidad, presencia, algoritmos de contenido y de adaptación para autogestionarse con sus únicas funciones, simplificando enormemente el diseño de tales plataformas.

La réplica y la distribución tienen significados muy distintos en el diseño y la gestión de un servicio del directorio. La ***réplica*** se utiliza para indicar que el mismo espacio de nombres de un directorio (los mismos objetos) está copiado en otro servidor de directorio por razones de redundancia y de rendimiento de procesamiento. El espacio de nombres replicado es gobernado por la misma autoridad. La ***distribución*** se utiliza para indicar los servidores de directorio múltiples, es decir, considerar diversos espacios de nombre interconectados para formar parte de un Servicio de Directorio distribuido. Cada espacio de nombres distinto puede gobernarse por diversas autoridades.

El Viaje de la Optimización de la Infraestructura

Analicemos ahora otro concepto importante. De acuerdo con los analistas, algo más del 65% del presupuesto normal de las Áreas de TI se invierte en infraestructura, tal como servidores, ambientes operativos, almacenamiento y gestión de conectividad. Si se le suma a lo anterior la necesidad de actualizar y administrar estaciones de trabajo y otros dispositivos de escritorio tendremos un conjunto único de desafíos a enfrentar asociado a la infraestructura de TI (en adelante ITI). (Microsoft, 2007)

El Modelo de optimización de infraestructura contribuye a colaborar a que los clientes dimensionen y consecuentemente mejoren el estado de su ITI; describiendo lo qué eso implica en términos de costos, seguridad (riesgos) y operatividad.

Antecedentes

La infraestructura TI es un activo estratégico y uno de los cimientos críticos sobre los cuáles el software puede ofrecer los servicios y las aplicaciones de usuario que necesita una organización para desenvolverse de manera efectiva y alcanzar sus objetivos. Para muchas organizaciones el crecimiento y el rápido desarrollo de nuevas tecnologías ha resultado en infraestructuras de centros de datos y de escritorio con alta complejidad, poco flexible y difícil de administrar con costos integrados que no sólo son altos, sino que de alguna manera son fijos sin importar si se modifican los requisitos de la organización.

La mayoría de las organizaciones reconoce la importancia de una ITI optimizada y rentable y ha 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, por citar alguna. Estas iniciativas realizadas por los departamentos de TI de manera aislada no son

suficientes por sí mismas para brindar las mejoras deseadas y a largo plazo que demandan las organizaciones. Para alcanzar una mejora sostenible en el tiempo en su ITI, las organizaciones deben definir una visión estratégica a más largo plazo respecto a la madurez esta infraestructura. Y vincular estas mejoras en capacidad y consolidación a sus objetivos y a la estrategia general de la misma.

Introducción al Modelo

El Modelo de Optimización de la Infraestructura fundamentalmente colabora a que las organizaciones alcancen importantes mejoras en costos para su infraestructura de TI al ir evolucionando desde un entorno no administrado a un entorno dinámico. La seguridad mejora de un estado “altamente vulnerable” en una infraestructura Básica a una seguridad “dinámicamente proactiva” en una infraestructura más madura. El concepto es que la administración de la ITI cambia de un estado “manual y reactivo” a un estado “automatizado y proactivo”.

El concepto es ir implementando las tecnologías, los procesos y procedimientos para ayudar a que la organización avance a través del viaje de la optimización de infraestructura. Los procesos cambian de “fragmentados o no existentes” a “optimizados y repetibles”. La capacidad de una organización para utilizar tecnología con el fin de mejorar la agilidad de su desempeño y ofrecer mejores servicios se incrementa conforme cambia de un estado “Básico” a un estado “Dinámico”. Capacitando a los trabajadores de la información y gerentes, y respaldando nuevas oportunidades de crecimiento.

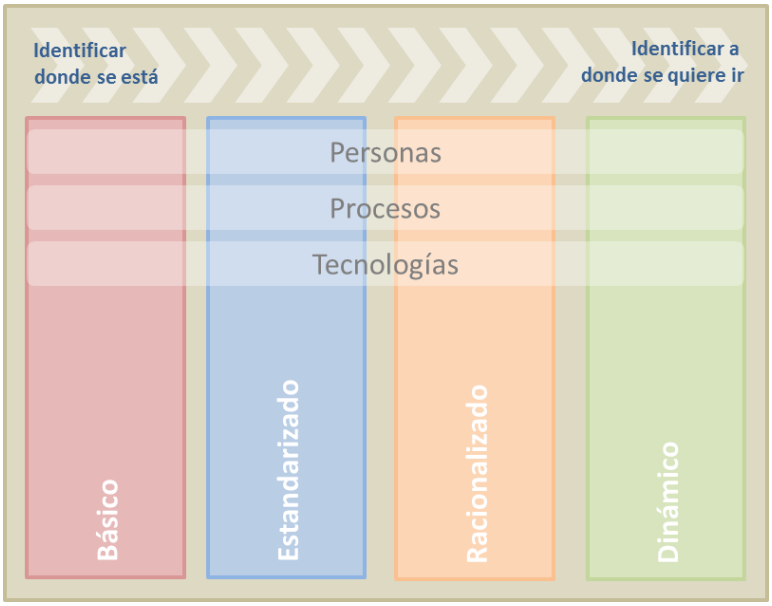

Ilustración 4. Viaje de Optimización de la Infraestructura.

Al trabajar con este modelo como esquema, una organización puede comprender rápidamente el valor estratégico y los beneficios que implica para la misma el cambiar de un nivel de madurez “básico” (donde la ITI por lo general es considerada un centro de costos) hacia un uso más “dinámico”, donde el valor que aporta la infraestructura de TI se puede comprender con claridad y se considera un activo estratégico de la organización y un habilitador de objetivos organizacionales.

¿Cómo funciona el Modelo?

El Modelo de Optimización de Infraestructura fue desarrollado empleando las mejores prácticas de la industria y la experiencia de Microsoft en su relación con el ambiente empresarial. Uno de los objetivos clave para los desarrolladores al crear este modelo fue desenvolver una sencilla manera de utilizar un esquema de madurez. A sí mismo, que fuera flexible y se pudiera utilizar con facilidad como la evaluación comparativa para la capacidad técnica y el valor en función de los objetivos organizacionales.

El primer paso, para utilizarlo, es evaluar en qué nivel de madurez se encuentra la organización dentro del modelo. Una vez que se establece el nivel de madurez actual (el punto de partida), el siguiente paso es emplearlo para desarrollar un plan sobre cómo progresar a través de cada nivel de madurez. De esta forma poder alcanzar el nivel objetivo que se requiere de acuerdo con las metas organizacionales.

Los 4 niveles que define el modelo

Nivel Básico: “Se atienden urgencias permanentemente”

La infraestructura Básica de TI se caracteriza por procesos manuales y localizados; un control central mínimo; y políticas de TI inexistentes o no aplicadas, así como normas relacionadas con la seguridad, respaldos, administración e implementación de imágenes, cumplimiento y otras prácticas comunes de TI. Existe una falta general de conocimientos relacionados con los detalles de la infraestructura con la que se cuenta actualmente o qué tácticas tendrán el mayor impacto para mejorar esto. Se desconoce la salud general de las aplicaciones y servicios, debido a la falta de herramientas y recursos. No existe un vehículo para compartir los conocimientos acumulados en el departamento de TI. Los clientes con infraestructura Básica encuentran que sus entornos son sumamente difíciles de controlar. Tienen costos muy altos de administración de escritorios y servidores, por lo general son muy reactivos a amenazas de seguridad, y tienen un impacto positivo muy pequeño sobre

la capacidad de aportar a los objetivos organizacionales para beneficiarse de la TI. Por lo general todas las revisiones, implementaciones de software y servicios se proporcionan a un alto costo.

Las organizaciones se benefician enormemente al cambiar de este tipo de infraestructura Básica a una Estandarizada, ayudándoles a reducir en gran medida los costos asociados a través de:

Desarrollar normas, políticas y controles con una estrategia aplicable.

Eliminar los riesgos de seguridad al desarrollar una postura de "defensa profunda": un enfoque en capas para la seguridad a nivel perímetro, servidor, escritorio y aplicación.

Automatizar gran número de tareas manuales, las cuales consumen un número elevado de horas-hombre.

Adoptar mejores prácticas, tales como aquellas de la Biblioteca de infraestructura de TI (ITIL), el SysAdmin Audit Network and Security Institute (SANS), por citar algunas.

Aspirar a convertir el departamento de TI en un activo estratégico en lugar de un costo.

Estandarizado: “Se comienza a obtener el control”

La infraestructura Estandarizada introduce controles a través del uso de normas y políticas para administrar los escritorios y servidores, cómo se introducen las máquinas a la red y el uso de los servicios de directorio para administrar los recursos, las políticas de seguridad y el control de acceso. Los clientes en un estado Estandarizado han logrado el valor de los estándares básicos y algunas políticas, sin embargo, siguen siendo un poco reactivos. Por lo general, todas las revisiones, implementaciones de software y servicios de escritorio se proporcionan a través de contactos de medios con costos de medios a altos. Sin embargo, cuentan con un inventario razonable de hardware y software y están comenzando a administrar las licencias. Se han mejorado las medidas de seguridad con un perímetro bloqueado, sin embargo, la seguridad interna sigue representando un riesgo.

Los clientes se benefician de cambiar de este estado Estandarizado a un estado Racionalizado con su infraestructura al obtener un control sustancial sobre la infraestructura y al tener políticas y procesos proactivos que los preparan para el

espectro de circunstancias desde oportunidades hasta la catástrofe. La administración del servicio es un concepto y la organización realiza los pasos para reconocer dónde implementarlos. La tecnología también está comenzando a desempeñar un rol más importante al cambiar hacia una infraestructura Racionalizada y convertirse en un activo estratégico y un aliado en lugar de un gasto.

Racionalizado: "Habilitamos los objetivos"

La infraestructura Racionalizada es donde los costos involucrados en administrar escritorios y servidores se encuentran en su nivel más bajo y los procesos y las políticas han madurado para empezar a desempeñar un rol importante en el soporte y la expansión de la empresa. La seguridad es muy proactiva y la respuesta a amenazas y desafíos es rápida y controlada.

El uso de la Implementación que requiere una mínima interacción del usuario en el sistema (conocido como "*zero-touch*") con pocas modificaciones; minimiza el costo, el tiempo de implementación y los desafíos técnicos. El número de imágenes es mínimo y el proceso para administrar escritorios requiere muy poca intervención del personal de TI. Tienen un inventario claro del hardware y software y compran sólo las licencias y PCs que necesitan.

La seguridad es en extremo proactiva con políticas y control estrictos desde el escritorio hasta el servidor y el firewall a la extranet.

Las organizaciones se benefician al cambiar de este estado Racionalizado a un estado Dinámico. Los beneficios de implementar tecnologías nuevas o alternativas para responder a los desafíos que presentan los objetivos u oportunidades superan por mucho los costos incrementales. Se implementa la administración de servicios para algunos servicios, ya que la organización realiza los pasos para implementar éstos con mayor amplitud en todo el Departamento de TI. Las organizaciones que contemplan el valor del estado Dinámico por lo general buscan que su infraestructura de TI proporcione una ventaja competitiva.

Dinámico: "TI es un activo estratégico"

Las organizaciones con una infraestructura Dinámica están totalmente conscientes del valor estratégico que proporciona su infraestructura al ayudarles a alcanzar sus objetivos de manera eficiente y al mantenerse competitivos. Los costos están completamente controlados. La integración entre los usuarios y los datos, escritorios y servidores y la colaboración entre los usuarios y los departamentos es

constante. Los usuarios móviles cuentan con niveles de servicio y capacidades casi en el sitio sin importar su ubicación.

Los procesos son completamente automatizados y con frecuencia se incorporan en la misma tecnología, permitiendo que el Departamento de TI esté alineado y sea administrado de acuerdo con las necesidades de la organización. Las inversiones adicionales en tecnología ofrecen beneficios específicos, rápidos y medibles en función de los objetivos organizacionales.

El uso del software de auto-aprovisionamiento y sistemas tipo cuarentena para asegurar la administración de revisiones y el cumplimiento con las políticas establecidas de seguridad permite que la organización dinámica automatice los procesos, mejorando así la confiabilidad, reduciendo los costos y elevando los niveles de servicio.

Los clientes se benefician al elevar el porcentaje de su infraestructura que es Dinámica al proporcionar mayores niveles de servicio, una ventaja competitiva y comparativa, y al resolver mayores desafíos de negocios. La administración de servicios se implementa para todos los servicios críticos con contratos de nivel de servicio y revisiones operativas establecidas.

Arquitectura de Referencia

Ante la realidad descripta, una organización debe considerar seriamente la necesidad de adoptar estándares; evolucionar hacia estos, para que le permitan tener la capacidad de adaptación. Variables como lo son la complejidad, el cambio, la innovación, costos sustanciales y demás, asociados a la rápida transformación de los ambientes tecnológicos representan un desafío a ser considerado muy seriamente. La eficacia significativa se presenta del hecho de no tener que reinventar la rueda y resolver reiteradamente los mismos problemas. Adoptar soluciones ya probadas y exitosas, se torna muy interesante y hasta vital. Esto nos permite ahorrar el tiempo valioso y a la vez escaso, para emplearlo en alcanzar los objetivos organizacionales. La propuesta de tender hacia entornos operativos (o “ecosistemas”), en lugar de ir hacia productos tecnológicos se presenta como una directriz. Es aconsejable ver las soluciones desde una visión global e integradora. Mirar más allá del corto plazo.

Desde hace años la tendencia tecnológica en TI, se ha orientado hacia el desarrollo de soluciones tecnológicas adaptables, integrables y con visión a más largo plazo. Así líderes de la industria como HP, SUN, Microsoft, e inclusive empresas del

mundo del software libre como creadores de distribuciones de LINUX, están desarrollando sus propias arquitecturas de referencia. Estas arquitecturas no solo involucran tecnología, además abarcan procesos y personas. Y esta es una de las mayores riquezas, y fortaleza esencial.

A continuación se describirá que debería involucrar una Arquitectura de Referencia (AR). Se desarrollaran conceptos que tienden a generar un marco sobre el cual será posible establecer relaciones entre las diversas arquitecturas existentes.

Objetivos de Diseño

Una arquitectura de referencia se debería plantear como un conjunto de guías que mayormente estén dirigidas a áreas funcionales dentro de la tecnología como pueden ser los Servicios de Directorio, Servicios de Mensajería, Servicios de Colaboración o Servicios de Archivos e Impresión por citar ejemplos.

Las guías son la base de diseño de la arquitectura. Se podría decir que es la mínima base indivisible de análisis. La arquitectura esencialmente es un conjunto de guías. Estas deberían contener diseños arquitectónicos, especificaciones, procesos, documentación, plantillas, modelos e información relevante para cada uno de los servicios o productos que la arquitectura engloba.

Sin embargo, hay otros aspectos fundamentales que se involucran en el diseño, particularmente a nivel de arquitectura, y que son necesarios de ser abordados. Estos aspectos son denominados “requerimientos no funcionales” y se describen a continuación:

- **Disponibilidad**: Cada componente de la arquitectura debe poseer una solución o estrategia para alcanzar la alta disponibilidad. Más que citar el conjunto de números 9s como porcentaje de disponibilidad, las guías deben apuntar a desarrollar la infraestructura de alta disponibilidad para reunir los requerimientos de la organización. Cada organización, en relación a su cultura organizacional, posee una definición diferente de disponibilidad. Por consiguiente, las guías proveen amplias soluciones técnicas y tecnológicas para combatir los tiempos no productivos (en inglés se conoce como *downtime*) cumpliendo con los objetivos pre-planeados.
- **Seguridad:** La arquitectura normalmente debería tender a beneficiarse de una estrategia conocida como defensa en niveles o capas, la cual es

un acercamiento abarcativo de aplicar seguridad integrando y alcanzando a toda la infraestructura. Es decir, ocuparse de vulnerabilidades de seguridad referentes a personal, tecnología y operaciones a lo largo de todo el ciclo de vida de la tecnología y los sistemas.

- **Escalabilidad:** Las estrategias de escalabilidad hacia arriba (en inglés *Scale-Up*) y escalabilidad hacia fuera (*Scale-out*) son específicas respecto al rol que juega cada componente en la arquitectura. Como ejemplo, Un motor de base de datos puede necesitar escalar hacia arriba para mejorar la performance y crecer y escalar hacia fuera con múltiples *clusters* para mejorar la performance y disponibilidad. Un componente como el servidor Web, basado en granja de servidores, sin embargo, es preferible que escale hacia afuera usando el balanceo de carga para proveer cambios rápidos y simples basados en la demanda.
- **Manejabilidad:** Poseer una solución de extremo a extremo (en inglés *end-to-end*) para despliegue, monitoreo, alertado, documentación y lectura de bitácoras (*logs*) y administración de la infraestructura, así como la gestión del despliegue del contenido.
- **Confiabilidad:** Soluciones confiables deben provenir de un comportamiento coherente y consistente que obedecen a la habilidad de desplegar reiteradamente arquitecturas y sistemas estandarizados.
- **Soportabilidad:** Todas las recomendaciones y configuración que acompañan la arquitectura deberían estar de acuerdo con la organización relevante de la ayuda para asegurar el grado más alto de soporte.
- **Repetitividad:** La arquitectura debería involucrar mecanismos de despliegue de soluciones ya probadas para alcanzar despliegues repetibles de una forma rápida y fácil.
- **Estandarización:** La implementación de componentes de infraestructura estandarizados a través de especificaciones arquitectónicas bien conocidas permitirá crear soluciones predecibles y confiables, y también proveerá bases para que la organización pueda manejar el cambio y el crecimiento.
- **Integrabilidad:** Una arquitectura tenderá a integrar productos de software y productos de hardware para formar una solución integrada que reúna las necesidades de la organización.

Desarrollo basado en modelos (Model-based Development)

Teniendo en cuenta volumen de las organizaciones sobre las cuales orientaremos el estudio, suele ser una muy buena práctica de modelado tratar de definir ciertos escenarios que nos permitan clasificar y comprender aún más las organizaciones. O quizás más que clasificar, comprender y/o dimensionar. Aquí se analizan los problemas específicos de las distintas áreas y los requerimientos de los objetivos organizacionales. Estos escenarios podrían ser generalizados para un amplio contexto a fin de asegurar que ellos engloben requerimientos en una manera consistente a través del ámbito de una organización típica. Así es posible hablar del "**modelo organizacional"**.

El Modelo Organizacional

Para asegurar su aplicabilidad, un modelo organizacional necesita ser una abstracción de diferentes tamaños, distribuciones, y con aspectos tecnológicamente dependientes de organizaciones típicas. Para este fin, una arquitectura debería comprender distintos conjuntos de escenarios que van a definir como los servicios dentro de las diferentes áreas de una organización serán implementados y ofrecidos. Se tomará como ejemplo de estudio una organización del tipo educativa como lo es una Universidad.

Se definen los siguientes escenarios:

- **Centro de Datos Centralizados (CDC):** Este escenario se define sobre el soporte a servicios de nivel organizacional para integrantes de la organización. Como ejemplo podemos citar algunos como mensajería, archivos e impresoras y Servicio de Directorio. El escenario CDC puede contener una presencia básica en Internet.
- **Departamento (DEP):** Un Departamento alberga la ITI necesaria que necesitan los distintos departamentos de la organización. Como ejemplo, una universidad dispondría de los departamentos de Personal, Alumnos, Biblioteca, entre otros. Esto representa una separación lógica dentro de la organización para propósitos de autonomía y dirección.
- **Unidades (UNI):** Provee un entorno físicamente descentralizado representando la distribución geográfica natural de la organización. Las unidades pueden tener servicios locales si el costo y la administración adicional lo justifican. Una unidad que no posee servicios locales se la denomina Unidad Satélite. Ejemplos de unidades podrían ser Institutos

de Investigación, Museos, Unidades Académicas geográficamente alejadas, entre otras.

- **Extranet (EXT):** Un entorno en el que los usuarios externos y personal interno acceden a los recursos y aplicaciones en forma segura, permitiendo el intercambio de información y colaboración. Este sería el caso de una implementación de EAD típica y pura.
- **Centro de Datos de Internet (CDI):** Diseñado para soportar un amplio conjunto de aplicaciones académicas, basadas en la Web que conecta a las organizaciones con sus usuarios**.**

Estos escenarios son una mezcla de entidades físicas y lógicas diferenciadas por necesidades geográficas, de aislamiento, de objetivos académicos o de independencia en el contexto de estructuras organizacionales típicas. La ilustración siguiente representa una estructura de organización que se separa en instalaciones académicas y regionales y una red de unidades basada en la disposición de servicios y de consumos. El escenario CDC (lo que podría de Rectorado) provee servicios para usuarios internos dentro de los campus regionales los cuales son lógicamente separados en departamentos; esto también provee servicios basados en intra y extranet. Una red de unidades típica es usualmente de gran alcance, emplea servicios de la organización, y está orientada a satisfacer necesidades puntuales de los usuarios.

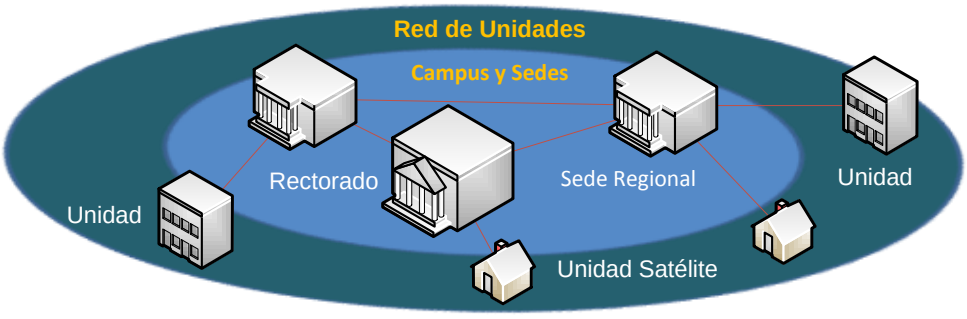

Ilustración 5. Distribución geográfica de escenarios.

El propósito de definir escenarios, basándose en un modelo organizacional, es poder brindar una herramienta para modelar una estructura organizacional. Ayuda a entender el proceso de proveer servicios a la gente que constituye la organización o que está en contacto con la misma. Por consiguiente, es conveniente definir claramente la perspectiva de cómo los docentes internos, personal de apoyo, docentes y usuarios externos, alumnos y demás consumen "servicios" desde las diferentes configuraciones. El propósito de estas configuraciones y su distribución dentro de la estructura organizacional es la de "proveer servicios". Este concepto, el de proveer servicios, es una de las directrices básicas a considerar. Esto nos ayudará a modelar una estructura organizacional, pensando en servicios, sobre los cuales aplicar las guías de diseño de los diferentes componentes que constituyen una arquitectura.

La tabla 2 provee una detallada descripción de los escenarios en el contexto de los consumidores de servicios TI de la organización y en la distribución de dicho servicios.

Consumidor	Escenarios	Propósito
Usuarios Internos	Centro de Datos Centralizado (CDC)	El escenario CDC provee a los empleados en una organización de esos servicios que son críticos para la operación de los objetivos de la misma. Para organizaciones globales, el CDC es una entidad lógica en el sentido de que puede ser implementada para proveer la distribución de servicios a un nivel geográfico extendido (continental) como así también en regiones importantes dentro de un continente que forma una jerarquía de la provisión del Servicio. También puede recibir la presencia básica de Internet cuando la función única de la organización no es solo Internet (en contraste con el CDI, definido más abajo). Los usuarios y servicios tienen requerimientos y restricciones alrededor de la administración, conectividad, seguridad y gestión.

	Unidad (UNI)	Muchas organizaciones, en nuestro caso Universidades, poseen varias Unidades que constituyen los puntos finales para el consumo de servicios. Algunos pueden albergar servicios localmente mientras que otras pueden que no, y todas poseen distintos anchos de banda y fiabilidad de conexión. Ellas pueden usar servicios desde localizaciones relevantes en la jerarquía hacia el CDC. El requerimiento fundamental es asegurar el acceso a los servicios principales de la organización. Las unidades sin servicios locales podemos definirlas como Unidades Satélites.
	Departamento (DEP)	El escenario de Departamento provee el ambiente seguro para computación necesario para departamentos o divisiones particulares dentro de la organización. Este escenario es usualmente aplicado para aislamiento o por razones de autonomía relacionado con aplicaciones sensibles o administración de infraestructura. La tecnología requerida para albergar las necesidades departamentales puede ser un entorno separado física o lógicamente. Como ejemplos podemos citar los Departamentos de Alumnos o Legales dentro de las Facultades los cuales poseen datos sensibles.
Usuarios Externos	Extranet (EXT)	Los escenarios de Extranet dan soporte a interacciones del tipo “Entre Pares” es decir entre organizaciones similares (Universidades o Ministerios de Educación) y entre estas y organizaciones diversas. Empleados de múltiples cátedras o Institutos de diversas Facultades o Universidades podrían acceder en forma segura a recursos y aplicaciones habilitándolos luego a intercambiar y trabajar en forma colaborativa dentro de un espacio de información compartida. La Extranet no solo mejora sustancialmente los procesos académicos de las organizaciones, sino que también provee la habilidad de conducir la formación en tiempo real con un gran número de actores.

Alumnos	Centro de Datos Internet (CDI)	Un CDI alberga servicios para actividades académicas basadas en Internet entre organizaciones y sus usuarios. Esta infraestructura dedicada y aislada es relevante para organizaciones donde la formación basada en internet constituye todo o una parte significativa de la organización. Estas organizaciones es probable que tengan un CDC, posiblemente con servicios extranet, para soportar las necesidades de los usuarios externos e internos. Estos Centro de datos son frecuentemente manejados por diferentes grupos de personas en las organizaciones debido a que ellos poseen distintos requerimientos para disponibilidad, seguridad y capacidad de crecimiento.

Tabla 2. Definición de escenarios.

Basándose en estas definiciones, una arquitectura debería entregar, como ya fue comentado, un conjunto de guías en evolución continua. Estas guías deberían contener diseños arquitectónicos, especificaciones, procesos, documentación, plantillas, modelos e información relevante basada en la prestación de servicios, y dentro de los escenarios descriptos. Los servicios son una mezcla de servicios TI y servicios de usuarios finales. A continuación se presenta una clasificación que podría definirse:

Servicios TI

- Servicio de Directorio.
- Servicio de Certificados.
- Servicios de Acceso Remoto.
- Servicios IP (WINS, DNS, y DHCP).
- Servicio de Cortafuego (FireWall).

- Servicios de Usuarios Finales
  - Servicio de Archivos.
  - Servicios de Impresión.
  - Servicio de Mensajería.
  - Servicio de Colaboración.

Estas guías deberían ser desarrolladas basándose en escenarios reales. Las actuales arquitecturas, tienden hacia esto. Sin embargo, no todos los usuarios pueden

necesitar consultar las guías desde la perspectiva de los escenarios. Algunos usuarios pueden estar interesados en un servicio en particular o en un conjunto de servicios que estén relacionados directamente con sus intereses o requerimientos de la organización. Para lograr esto, las guías deberían publicarse bajo un enfoque modular por medio del cual las dos vistas se pueden lograr. La vista basada en escenario y la basada en servicio. A continuación se muestra la ilustración que permite comprender gráficamente el planteo de las dos vistas

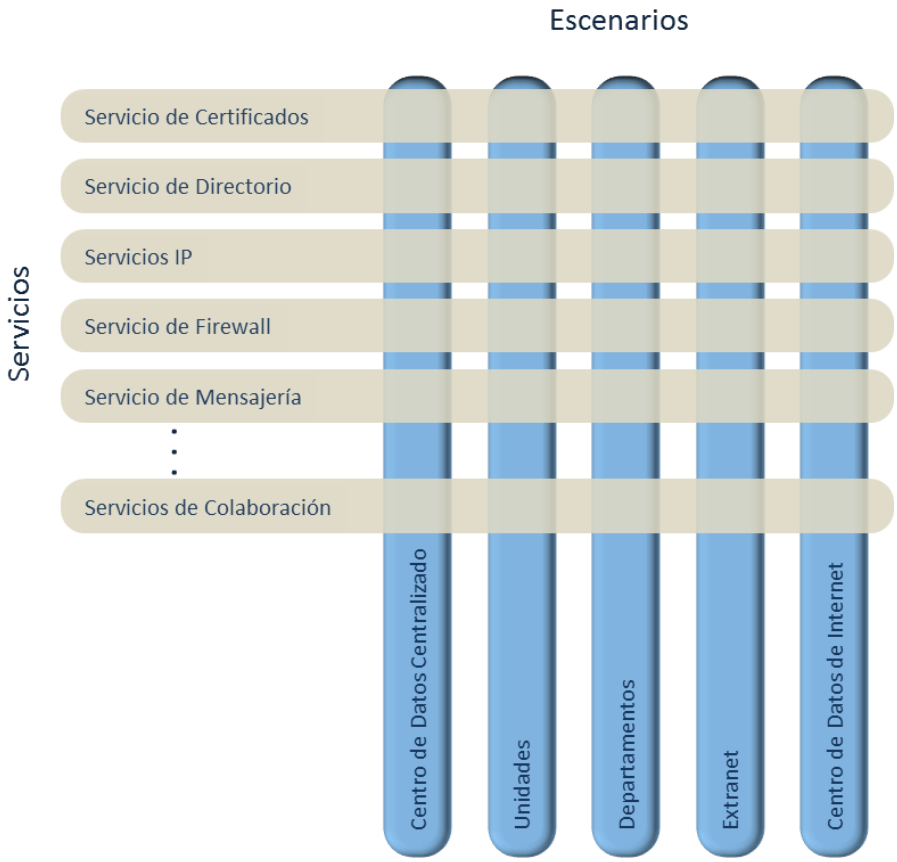

Ilustración 6. Vistas basadas en Escenario y basadas en Servicio.

Aportes de una Arquitectura de Referencia

Adecuación a las necesidades

Cada organización posee requerimientos particulares que no pueden ser satisfechos exclusivamente mediante la adopción o aplicación de una arquitectura. Naturalmente, en base a la perspectiva y experiencia de años, y a través de una dirección paso a paso será posible cumplir con los mencionados requerimientos. Las guías de las arquitecturas deberían ser diseñadas y desarrolladas con el conocimiento

que cuando es adoptada, requerirá adecuaciones para alcanzar los requisitos particulares y únicos fijados en los objetivos organizacionales. También debería considerarse el condicionante que representa la tecnología asociada propiedad del usuario. La documentación que conforma la arquitectura no debería ser desarrollada como una solución universal para todos los casos, sino como un conjunto de opciones de diseño y de mejores prácticas que pueden ser usadas para implementar una solución particular; entender que decisiones están disponibles para el usuario, porque una decisión debe ser tomada en un escenario determinado y como se implementa esa solución. Como tal, la documentación debería ofrecer la información de integración de tecnología que se haya probado a fondo para resolver metas arquitectónicas específicas de disponibilidad, seguridad, escalabilidad, y manejabilidad.

Cuántas veces en un proyecto de TI alguien dice o lo presiente, "Esto se ha hecho seguramente antes", y cuántas veces las ruedas siguen reinventándose, produciendo esencialmente soluciones idénticas a los desafíos comunes de la infraestructura. Una arquitectura debería tratar estos temas proveyendo una infraestructura estandarizada, pre-comprobada y con soluciones listas para implementarse basándose en los escenarios típicos. Esto permitiría que el cliente o el integrador de sistemas se centren solamente en los aspectos de su proyecto que sean únicos. Aquello que lo diferencia de los demás, y lo identifica.

Una arquitectura tendría que tener la intención de ser un punto de partida para que los usuarios inicien en forma rápida sus proyectos de infraestructura TI. Los diseños de referencia permitirían tomar decisiones de diseño basadas en opciones bien descriptas y en sus propios requisitos únicos. Las guías de implementación complementarían los diseños de referencia permitiendo la integración de tecnologías basadas en situaciones bien conocidas y previamente probadas.

Aquí es oportuno recordar la Ilustración 1. Ventajas de basarse en una Arquitectura de Referencia, al inicio en la justificación. Esta ilustración represente una comparación de un proyecto de infraestructura TI usando una arquitectura (Basado en AR) de uno que no la usa (Tradicional). En el eje vertical es posible ubicar la variable tiempo, esfuerzo o complejidad.

En esta comparación, se puede asemejar al proyecto que adoptó una metodología de desarrollo tradicional con el hecho de construir una casa sin un diseño o un modelo previo; requiere más trabajo satisfacer los requisitos particulares para alcanzar las mismas metas que el proyecto que se basó en una AR. Es más fácil partir de planos o

modelos pre-probados de una casa tipo para satisfacer las necesidades de un proyecto que empezar desde cero. Comenzar un proyecto usando la guía de una AR permite a una organización materializar los siguientes beneficios en una forma más rápida:

- **Alcanzar en menos tiempo las condiciones de puesta en servicio**: le toma menos tiempo completar un proyecto cuando las adecuaciones particulares son mínimas.
- **Reducir riesgos:** reduce los riesgos usando los diseños bases probados de la Arquitectura.
- **Reducir costos:** La solución tiene menor costo ya que requiere menores adecuaciones particulares para alcanzar las necesidades particulares de cada usuario.
- **Reducir complejidad:** la complejidad tiende a ser controlable. Se parte de soluciones bien detalladas y conocidas.
- **Enfocar el esfuerzo en lo relevante:** mediante el seguimiento de las guías de la arquitectura, se alcanzan rápido las metas de lo ya conocido, fara enfocar el esfuerzo en lo particular de la organización. Aquello realmente importante.

Diversos aspectos de un proyecto que requieren adecuaciones particulares involucran sin duda algo de disponibilidad, seguridad y escalabilidad. Una consideración importante en lo que a disponibilidad se refiere es conocer el grado de tolerancia de las necesidades de una organización a potenciales puntos de falla. Las AR deberían ser diseñadas y probadas bajo el estándar o concepto conocido como “sin único punto de falla” (NSPoF, en inglés N*o Single Point Of Failure*).

Los objetivos primarios de las organizaciones pueden variar. Esto es normal por diversos factores, que suelen ir desde lo cultural hacia lo económico o financiero por citar ciertos aspectos. Una organización puede entender y estar dispuesta a aceptar los riesgos asociados a no desplegar todas las tecnologías NSPoF específicas. En tal caso, el despliegue gradual de tecnología, productos, servicios y demás correspondientes al proyecto se puede considerar apropiada y por lo tanto acertado para los objetivos organizacionales o del proyecto.

Ahora bien, la adecuación por requisitos particulares es inevitable y necesaria. Un punto fundamental del valor de las ARs es que deberían consistir en configuraciones probadas previamente que hayan demostrado su operatividad. Esto reduciría riesgos, costos y tiempo para entrar en la tan ansiada fase de producción. Por lo tanto, cada adecuación para requisitos particulares debe ser evaluada cuidadosamente para comprender cómo afectaría. Los costos, riesgos, y el tiempo adicionales requerido para el desarrollo de pruebas adicionales se deben aceptar en su debida medida e incluirlos en la decisión final para la adecuación de la arquitectura.

Es aconsejable asumir que puede haber una lista relativamente significativa de arreglos para requisitos particulares que deben ser considerados. Una alternativa sana y quizás aconsejable, es que profesionales con la experiencia suficiente y el conocimiento integral de la arquitectura ayuden a la “adecuación” en base a la misma

Estandarización

La documentación de una arquitectura debería ser el estado final óptimo (deseable) para la infraestructura TI referida. En consecuencia, se podría presentar como un estándar que puede ser usado por parte de las organizaciones. Este estándar puede ser empleado por la organización en una variedad de formas. En el amplio espectro, la documentación de una arquitectura puede ser utilizada o aplicada como un punto de referencia alrededor de la gente, de procesos, y de la tecnología subyacente para obtener beneficios específicos de las interacciones entre ellas.

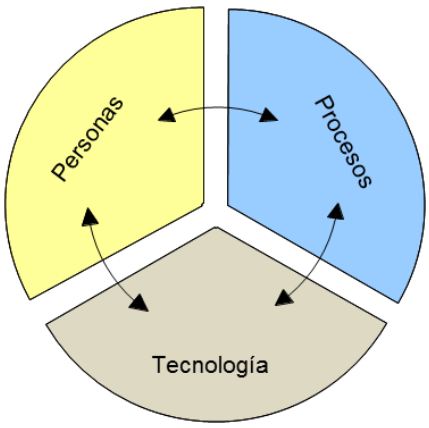

Ilustración 7. Interacción entre Personas, Procesos, y Tecnologías.

Personas y Tecnología

Históricamente, ha habido problemas entre las necesidades u objetivos organizacionales que los desarrolladores de aplicaciones manejan y la infraestructura en la cual las aplicaciones residen. La fricción proviene de una carencia de un común denominador o estandarización al diseñar, construir, desplegar, y operar aplicaciones e infraestructura. Cuando se acuerda un proyecto, los equipos de aplicaciones e infraestructura pueden crear un entendimiento común de cómo apoyarse el uno en el otro y asegurar consistencia a través de una solución completa. Los desarrolladores de aplicaciones han necesitado largamente una infraestructura TI estándar, y los modelos basados en arquitecturas se pueden utilizar para crear estos acuerdos entre los profesionales de infraestructura y los desarrolladores de aplicaciones. Tales acuerdos beneficia a los desarrolladores proporcionando una infraestructura que apoye sus requisitos. Además, la infraestructura TI basada en una arquitectura tiende a ser optimizada para permitir ejecutar las aplicaciones en un ambiente de producción. Por lo tanto, los beneficios en TI se maximizan usando los estándares previamente convenidos.

Tecnología y Procesos

Los profesionales TI puede confiar en la arquitectura para asegurar la integración en la organización de las diversas tecnologías, ya sean propias de la organización como lo pueden ser las exteriores o de 3^{ros}. Lo anterior no solamente en las tecnologías específicas que la arquitectura de referencia incorpora, sino también en los procesos derivados en diseñar, construir, y operar las tecnologías en la organización. La aplicación de una arquitectura crea la colaboración entre la gente y la tecnología cuando estos crean y validan cada configuración que se define en la misma. Las guías subyacentes en el modelo de la arquitectura directriz proporcionan los principios que se ocupan específicamente de la seguridad, del establecimiento de una red, de la gerencia, de la infraestructura de aplicación, del almacenamiento, entre otros. Dentro del modelo de una arquitectura y de las guías preceptivas, hay un innumerable número de mejores prácticas en opciones de diseño de la tecnología, despliegue, y los procesos operacionales sobre los cuales pueden dibujar los profesionales de TI para crear los principios específicos a su organización.

Procesos y Personas

La documentación que acompaña a las arquitecturas, así algunas de ellas son muy detalladas en esto, brinda soporte a los profesionales a través del ciclo de vida de la TI. La documentación de una arquitectura se escribe para audiencias específicas y relevantes y trata los diversos requerimientos a través de su ciclo de vida. Es deseable

que una arquitectura ensamble lineamientos de estandarización proporcionando el marco para crear las guías para las fases de planificación, construcción, despliegue y operación del ciclo de vida. El programa que involucra una arquitectura aspira a proporcionar un interfaz consistente para comunicar esta guía a sus lectores; creando documentación que trata el diseño, la construcción, y la estructura de funcionamiento de la organización, constantemente como un método para lograrlo.

Beneficios

La propuesta de valor de una arquitectura de referencia es que proporciona un marco referencial para dirigir la fase de planeamiento de la Infraestructura TI basándose en escenarios organizacionales. Otro aporte es la posibilidad de repetir la solución con la certeza que ya ha sido construida en ambiente de laboratorio, integrado con tecnologías existentes, y pre-comprobadas. Permitiendo así una puesta en funcionamiento más ágil, con costos predecibles, riesgos reducidos, y asegurando un menor tiempo para alcanzar los beneficios. El programa de una arquitectura ofrece ventajas competitivas adicionales significativas, como son:

- **Un mapa guía y una visión de gran alcance para proteger la inversión en TI**: Una arquitectura debería ser un factor contributivo para una organización que desarrolle un entorno de operaciones estándar sobre el cual todas las soluciones e infraestructura se desenvolverán.
- **Prueba e integración**: Los escenarios que aportan las arquitecturas deberían ser rigurosamente probados en laboratorios que involucren tecnologías existentes. Además, aportando pruebas del mundo real en lo referente a costos de despliegue, mantenimiento y a la capacidad para alcanzar los niveles de servicios requeridos.
- **Costos controlados y conocidos con un funcionamiento previsible y más confiable**: Las configuraciones probadas en laboratorio deberían ser confiables, rápidas de desplegar, y proporcionar un costo total de propiedad (TCO) más bajo. Un conjunto de “materiales” predeterminados, métricas de funcionamiento conocidas, y guías de implementación reducen dramáticamente los costos de implementación.
- **Flexibilidad en la implementación y la integración**: Las organizaciones lograrían integrar con sus ambientes existentes y productos, configuraciones e implementaciones estándares de la industria.

- **Una guía para la reingeniería**: También es factible, de hecho comúnmente se realiza, emplear a la arquitectura como una base referencial para repensar los procesos y servicios internos y externos que la TI involucra.

El empleo de una arquitectura produce el despliegue de Infraestructuras TI confiable y segura con visión de futuro. Es una buena práctica que estos puntos sean observados con detenimiento. Las configuraciones basadas en arquitecturas también deberían entregan cinco ventajas técnicas dominantes al área responsable de la toma de decisiones en TI. Estos son quienes tienen la responsabilidad de asegurarse que el ambiente de funcionamiento de la infraestructura trabaja según lo esperado. Las ventajas técnicas asociadas son:

- **Guías:** Las guías de planificación, despliegue y operación que involucran el ciclo de vida TI. Habitualmente las arquitecturas se presentan mediante guías, las cuales suelen abarcar los servicios esenciales de la infraestructura.
- **Disponibilidad:** la arquitectura ayuda a alcanzar la redundancia o especialización funcional que limitan las fallas relacionadas a los sistemas.
- **Seguridad:** Las arquitecturas proveen un modelo de seguridad que se conoce como de “extremo a extremo” (en inglés *end-to-end*) que protege los datos y la infraestructura de ataques y robos maliciosos tanto externos como internos.
- **Escalabilidad:** Todos los componentes pueden ser escalados para proveer un crecimiento continuo para alcanzar las demandas de los usuarios y los requerimientos involucrados en los objetivos organizacionales.
- **Administrabilidad:** Facilidad de configuración, de supervisión de lo que se conoce como “la salud en curso”, y de la detección de fallas para anticiparse con el crecimiento del entorno.

CAPITULO III: SOLUCION PROPUESTA

CASO DE ESTUDIO

Definición de una Organización Mediana.

Desde el punto de vista del medio ambiente, y de la realidad existente, consideraremos establecer cierta analogía con la clasificación de PyMEs. Pero, en lo relacionado con este estudio, consideraremos la salvedad de darle un mayor peso a aspectos como volumen organizacional, complejidad de tecnología asociada y RRHH en las áreas TI (por citar algunos); por sobre los indicadores económicos y financieros. Lo anterior plantea dejar de lado el vocablo “empresa” para emplear el de “organización”. De este modo también abarcamos organizaciones sin fines de lucro, organizaciones gubernamentales, universidades y demás de características similares.

Si se toma la sigla PyME queda bastante claro el subconjunto o clasificación de empresas al que se está refiriendo. Como base para este estudio emplearemos la sigla “OM”, la cual significará Organización Mediana. Y componiendo podríamos definir la clasificación de Pequeñas y Medianas Organizaciones, cuya sigla sería PyMO. Las OMs, son organizaciones con características distintivas, que poseen dimensiones determinadas por límites a nivel de RRHH y recursos financieros entre otros. Las OMs son entidades con una cultura, lógica, intereses y espíritu emprendedor específico. Lo anterior las determina y sobre todo las identifica, les da identidad. A lo largo del capítulo iremos analizando características que nos permitirán ir definiendo con mayor claridad que organizaciones se pueden agrupar dentro de la clasificación de OM.

Importancia de este tipo de organizaciones.

Las pequeñas y medianas empresas, cumplen un importante papel a nivel social y del desarrollo del medio ambiente organizacional. De hecho este estudio ha tomado bases fundamentales de modelos, clasificaciones y números de ambientes donde se maneja información de las PyMEs. Un ejemplo de la importancia de este nivel de empresas es que los países de la OCDE (Organización para la Cooperación y el Desarrollo Económico) suelen tener entre el 70% y el 90% de las fuerzas laborales en este grupo de organizaciones.

Explorando en la estructura económica de distintos países, podemos encontrar sectores más dinámicos que otros, actividades que cuentan con ventajas comparativas frente a otros países. Pero en todos encontraremos empresas pequeñas, medianas y grandes.

Por otro lado en la actual economía mundial se observa claras tendencias hacia la internacionalización de los negocios y de los mercados. La liberación del comercio, el intercambio entre grandes bloques económicos regionales. Dentro de este proceso entendemos que las Pymes deben cumplir un papel destacado. Debido a la nueva concepción de la competencia, cobra especial relevancia el criterio de " especialización flexible" que contempla la capacidad de las empresas para responder en la forma adecuada a los cambios en el mercado internacional, adaptándose a los tipos de bienes producidos, cantidad y calidad de mano de obra, insumos y demás. Hasta el mismo proceso productivo debe replantearse.

Las PyMEs en este contexto encuentran su razón de ser, ya que constituyen las organizaciones más capaces de adaptarse a los cambios tecnológicos y de generar empleo. Por lo anterior representan un importante factor de política de distribución de ingresos a las clases media y baja, con lo cual fomentan el desarrollo económico de toda una Nación.

La importancia de las PyMEs es algo reconocido a nivel mundial. En este trabajo no se pretende dar una justificación al respecto, sino solamente citar estos puntos tratando de clarificarlos. De esta forma queda claro que cualquier implementación o desarrollo de tecnología que se aplique en esta franja de organizaciones, será algo de significativa importancia.

Clasificación de PyMEs en la Argentina y en otros países

Analicemos el siguiente cuadro comparativo, el cual presenta la clasificación de las empresas en Argentina por las ventas anuales y según el Sector. La clasificación depende del siguiente esquema de ingresos anuales sin impuestos (en pesos argentinos). (Ministerio de Industria, 2013).

Tipo de empresa	Sector				
	Agropecuario	Industria y Minería	Comercio	Servicios	Construcción
Microempresa	$610.000	$1.800.000	$2.400.000	$590.000	$760.000
Pequeña Empresa	$4.100.000	$10.300.000	$14.000.000	$4.300.000	$4.800.000
Mediana Empresa	$24.100.000	$82.200.000	$111.900.000	$28.300.000	$37.700.000

Tabla 3. Ingresos anuales de las PyMEs sin impuestos en Argentina.

Este cuadro es una referencia importante a la hora de considerar los montos anuales que maneja una Organización Mediana. Es decir que se puede manejar una relación entre una Empresa mediana y una organización del mismo tamaño. Estos montos determinan con cierta claridad el nivel de inversiones que son posibles de destinar desde las organizaciones a las distintas áreas y en especial al área de Ti que es central para este estudio.

Con la finalidad de ofrecer una visión más amplia acerca de la clasificación del tamaño de las empresas, se expone a continuación la aprobada por el Instituto Nacional de Estadística y Estudios Económicos, en Francia (INSEE); la Small Business Administrations, de Estados Unidos (SBA); la Comisión Económica para América Latina (CEPAL); la revista mexicana de Ejecutivos de Finanzas (EDF), la Secretaría de Economía de México (SEM), y finalmente la publicación "La nueva definición de PyME" de la Comisión Europea. Todas estas instituciones están dedicadas al fomento y desarrollo de las empresas en cada uno de sus países.

Institución/Publicación	Tamaño de la empresa	Números de trabajadores
INSEE Instituto Nacional de Estadística y Estudios Económicos - Francia	Pequeña	De 50 a 250
	Mediana	De 250 a 1000
SBA The Small Business Administrations- Estados Unidos	Pequeña	Hasta 250
	Mediana	De 250 a 500
CEPAL Comisión Económica para América Latina	Pequeña	Entre 5 y 49
	Mediana	De 50 a 250
EDF Revista mexicana de Ejecutivos de Finanzas	Pequeña	Menos de 25
	Mediana	Entre 50 y 250
SEM Secretaría de Economía – México	Pequeña	De 16 a 100
	Mediana	De 101 a 250
Comisión Europea Publicaciones de Empresa e Industria "La nueva definición de PyME"	Pequeña	Menos de 50
	Mediana	Menos de 250

Tabla 4. Clasificación del tamaño de las empresas.

Ahora bien, una de las variables que usaremos para dimensionar un rango de clasificación, es el determinado por el número de PCs que posee la organización. Se entiende que existe una relación entre la cantidad de PCs y la cantidad de empleados o agentes. En nuestro estudio se define que esa relación es aproximadamente cercana a 1 a 1. Es decir que se estima que por cada empleado de la organización existe una PC. Entonces, teniendo en cuenta lo anterior, definiremos que una OM es una organización con un número de entre 50 a 500 PCs. De esta forma se define el

subconjunto de organizaciones sobre el cual trabajaremos. Es decir estamos definiendo parte de la dimensión de nuestro caso de estudio.

Infraestructura Informática de una organización mediana

Modelo 3 + 1

La infraestructura informática de una empresa mediana debería ofrecer varios servicios para resolver las necesidades específicas de los objetivos de la misma. Definiremos un subconjunto de infraestructura informática como "*infraestructura central*" la cual se implementa para dar soporte al resto de la infraestructura informática, y no para resolver directamente necesidades asociadas a los objetivos principales de la organización (Microsoft, 2010). La infraestructura central enmarca el conjunto esencial de los componentes de infraestructura tecnológica de quienes dependen los demás servicios y que sería deseable implementar en cada organización mediana con desarrollo informático. Todos los servicios que no forman parte de la infraestructura central los enmarcaremos dentro de lo que se define como "*infraestructura complementaria*". La infraestructura complementaria se implementa para resolver exclusivamente las necesidades específicas asociadas a los objetivos organizacionales y deberán implementarse en función de la demanda que determine la realidad organizacional. En este punto es muy útil tener definido el nivel de optimización de la infraestructura en el cual se encuentra la organización, y el camino a seguirse al respecto.

No está dentro del alcance de este estudio el diseño de la infraestructura central para una organización mediana, pero con la idea de modelado, se presentará un diseño típico aconsejable para empresas medianas. Este quizás sea el diseño más simple y apropiado para comenzar con el desarrollo TI dentro de la organización. Este consiste en la distribución de servicios en componentes físicos. Se puede partir de tres o cuatro servidores distribuidos de la siguiente forma:

- **Servidores de infraestructura (cantidad = 2)**: Estos dos servidores ejecutan el ambiente operativo seleccionado por la organización y ofrecen servicios esenciales. Ambos se emplean para implementar la tolerancia a fallas para los servicios de red como son: DHCP, DNS (o similar), así como para dar soporte a un Servicio de Directorio. Estos servicios de suelen alojar en ambos servidores, respetando las modalidades de tolerancia a fallos que corresponde en cada caso.
- **Servidor de seguridad (cantidad = 1. Seguridad / Borde)**: puede ser un servidor o una implementación de un equipo dedicado (*appliance* o

blackbox). Es interesante la posibilidad de interacción que posea este equipo con el Servicio de Directorio implementado. Esto permitirá un desarrollo de la seguridad más granular, integrado y adaptado a la organización. Generalmente en este equipo se implementaran los servicios de cortafuego (firewall), delegado (proxy) y VPN.

- **Servidor de archivos y almacenamiento**: de manera opcional, se puede desplegar un dispositivo de almacenamiento unido a la red para ofrecer servicios de archivos y almacenamiento centralizado de datos. Quizás también una primera instancia de servidor de aplicación.

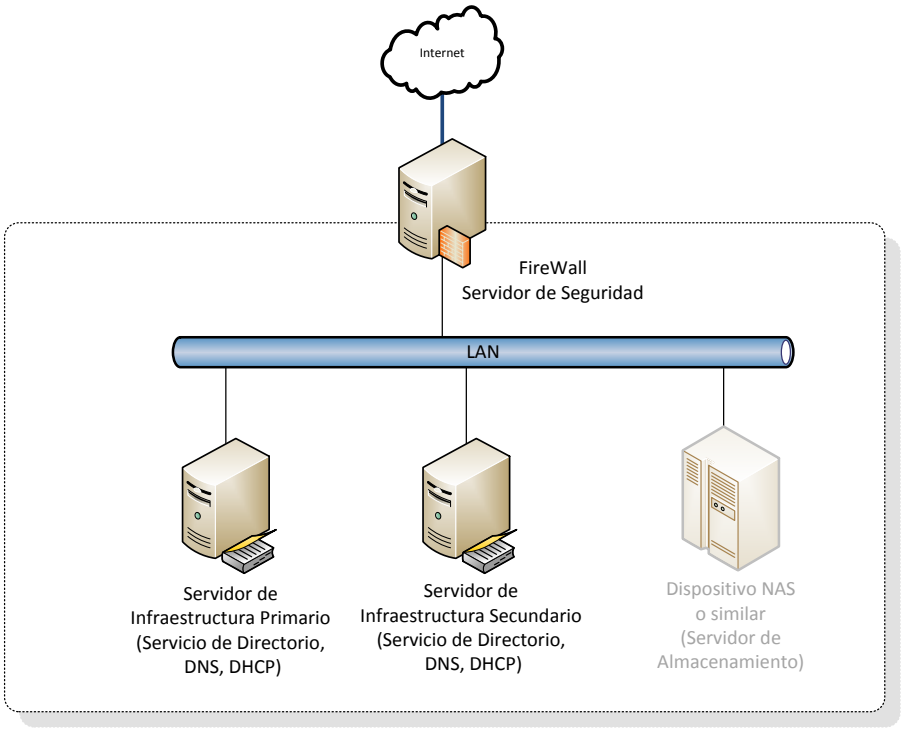

Ilustración 8. Infraestructura Central – Modelo 3 + 1.

Así, definiremos esta configuración “3+1”.

Como complemento, además de los servicios descriptos, este modelo presenta la posibilidad de implementar servicios adicionales en los dos servidores de infraestructura. Estos servicios adicionales pueden formar parte de la infraestructura complementaria, tales como mensajería, colaboración, entre otros. Decidir qué servicios adicionales alojar en los servidores de infraestructura depende de las necesidades y objetivos organizacionales como pueden ser necesidades de rendimiento, presupuesto, entre otros.

Infraestructura complementaria

Se presentan en forma de tabla una descripción de los servicios que se plantean a nivel de diseño abarcados por la infraestructura complementaria.

Solución	Descripción
Administración y seguridad basada en un Servicio de Directorio	Servicio para la administración y la seguridad de las estaciones de trabajos en un ambiente de informática mediano utilizando las configuraciones de políticas en general y una estructura de unidades organizacionales que puede aplicar a la mayoría de las empresas medianas.
Mensajería	Permite enviar mensajes (SMS, mail, fax) incluyendo como ejemplo el acceso remoto a correo electrónico, calendario, agenda, chat y tareas.
Colaboración	Permite el uso compartido de documentos e información similar de manera interna, lo que se conoce como Intranet. Y a través de sitios Web o accesos externos en lo conocido como extranet.
Cliente / escritorio	Permite la configuración de PCs, dispositivos y puntos finales de cliente en el ambiente de informática mediano.
Respaldo y recuperación	Permite planear la protección de datos utilizando una combinación de hardware como lo son los niveles RAID, servicio de Instantáneas de volúmenes y software de respaldo/recuperación.
Administración de revisiones / parches	Permite la implementación de revisiones/actualizaciones a nivel de Sistemas Operativos, servicios y aplicaciones. Así también es posible administrar las secuencias de versiones de las actualizaciones desplegadas.
Impresión	Permite implementar servicios de impresión y copias en el ambiente de informática mediano.
Conectividad remota	Permite el acceso remoto seguro al ambiente de informática mediano.
Seguridad de punto final	Permite el despliegue de soluciones para protegerse contra virus, correo no deseado, software espía y otros software maliciosos.

Tabla 5. Infraestructura Complementaria.

Definición de nuestro caso de estudio

Adoptaremos el modelo de Centro de Datos Centralizados (CDC), con la posibilidad de manejar Unidades, las cuales podrían ser satélites. Lo anterior es en base a lo expuesto en el capítulo de Antecedente o Marco teórico. La OM que definiremos como base de estudio (nuestro modelo), se puede desenvolver siguiendo los lineamientos producto de la unión de ambos modelos. Complementariamente y como base directriz, se empleará una arquitectura de referencia para ir planteando el desarrollo de la solución de Servicio de Directorio propuesta.

La organización poseerá una cantidad de agentes que puede variar desde 50 a 500 aprox. Y estará sustentada tecnológicamente sobre una infraestructura TI de 3 + 1 como lo definimos anteriormente.

Y en consecuencia, luego de la implementación del Servicio de Directorio siguiendo los lineamientos del presente trabajo, se sentarán sólidas bases para elevar

en un nivel la maduración de la organización según el modelo de Optimización de la Infraestructura. Pudiendo estar cerca del nivel estandarizado (Ilustración 4).

ALTERNATIVAS DE SOLUCIÓN

Analizando lo planteado, surge naturalmente la decisión de implementar un Servicio de Directorio. De las numerosas soluciones de servicios de directorio existentes que fueron enunciadas en el punto “Desarrollos de SDs” incluido en “Antecedentes y marco teórico”, resulta compleja la toma decisiones. Un SD, es un servicio transversal. Seguramente será necesario integrarlo, o definirlo como la base aglutinante de los diversos sistemas y servicios existentes en la organización. Un Servicio de Directorio debería estar íntimamente ligado con la mayoría de las soluciones tecnológicas, por lo cual se transforma en una solución extremadamente personalizada desde el punto de vista organizacional. Hay diversos aspectos que se deben tener en cuenta. Uno de estos es la experiencia del personal técnico informático. Otro es La base operativa que se emplea (NOS). Las aplicaciones que constituyen los sistemas de la empresa también constituyen un factor determinante. Otra posibilidad es definirse entre soluciones de directorio propietarias o de licenciamiento libre. No es el espíritu de este trabajo llevar a cabo un análisis comparativo, ni determinar un ganador luego de completar una extensa tabla comparativa de propiedades de los servicios de directorio. Los criterios son diversos, producto naturalmente de la “personalidad” de cada organización.

Así es claro que la decisión de implementar un SD es algo extenso y complejo. Que toda aplicación de TI dentro de la organización debería interactuar con el SD desplegado, tampoco debería discutirse. Que todo desarrollo futuro de software debería vincularse con el SD, debería también ser una de las premisas de las políticas de TI de las organizaciones.

Como experiencia del autor, habría 3 soluciones de SD que podrían tomarse como base para analizarse en la implementación a nivel de una Organización Mediana. OpenLDAP como solución si existe la decisión de inclinarse por el software libre. Y eDirectory de Novell y Active Directory de Microsoft, de existir la posibilidad de una solución propietaria o licenciada.

JUSTIFICACIÓN DE LA ALTERNATIVA

En este trabajo se toma la decisión de emplear el producto de Microsoft, Active Directory (AD). Como ya se expresó no está en el espíritu del mismo llevar a cabo un análisis comparativo. Pero en el contexto de una organización mediana, esta solución es una de las más desarrolladas en relación al conjunto de servicios y el nivel de integración con el resto de la infraestructura TI. Microsoft ofrece uno de los conjuntos más amplios de productos, para la administración y operación de TI que existen en la actualidad. En especial si se implementa AD sobre la plataforma de Windows 2008 R2, la cual administra los componentes del Servicio de Directorio como roles. En forma complementaria desarrolla documentación específica de cada servicio, lo cual facilita enormemente la evolución y operación del ciclo de vida de los servicios implementados. Esta documentación debidamente administrada conforma una base cierta que se puede emplear como base para iniciar la definición de una arquitectura de referencia. (Ver “Arquitecturas de Referencia” en el punto “Antecedentes y Marco Teórico”).

En un entorno TI de “informáticos generalistas” (término definido anteriormente en la “Descripción General del Problema”), esta solución representa un entorno altamente integrado sobre el cual es posible crecer con niveles concretos cohesión. Si bien AD está desarrollado para ser una solución corporativa para grandes organizaciones, se adapta perfectamente para organizaciones de nivel intermedio.

Lo expuesto no define que esta solución de Servicio de Directorio sea mejor o peor que otras. La implementación del Servicio de Directorio de Novell eDirectory también es muy completa, y con muy buena adaptación a organizaciones de mediano porte. Y dependiendo de los requerimientos específicos, la implementación de OpenLDAP es una alternativa válida.

Resumiendo, la solución de AD de Microsoft nos permite trabajar en un entorno de alta integración con los restantes servicios de TI en una organización mediana con un nivel de maduración estandarizada (en base al modelo de optimización de la infraestructura). La escalabilidad en cuanto al servicio es completa. Existe una arquitectura de referencia que los contiene, definiéndolo casi como estándar a nivel de servicio.

Por lo expuesto, se empleará AD de Microsoft para desarrollar el presente trabajo, no teniendo una dificultad mayor poder establecer relaciones comparativas u operativas con soluciones similares.

PROPUESTA

Contenidos

A continuación se detallan los contenidos que se cubrirán en el desarrollo de esta propuesta:

I. Introducción al Diseño y Planificación de un Servicio de Directorio.

II. Active Directory en la optimización de la Infraestructura según Microsoft.

III. Escenario donde aplicar.

IV. Requisitos Lógicos para el Diseño Arquitectónico

V. Proceso de diseño de Active Directory.

VI. Conclusiones.

VII. Posibles ampliaciones

Introducción al Diseño y Planificación de un Servicio de Directorio

Para llevar a cabo el desarrollo y conseguir un buen diseño de un directorio, en este caso Active Directory, es necesario contemplar numerosos aspectos interrelacionados. Lo citado es a fin de obtener respuestas ciertas a numerosas preguntas. Muchas decisiones y estrategias deben ser determinadas y definidas. Se deben analizar consideraciones relacionadas al rendimiento, respecto a la seguridad, manejabilidad, escalabilidad, y numerosos criterios que deben abordarse para obtener un diseño exitoso.

Este trabajo se presenta como una guía a diseñadores en la toma de decisiones. Se intenta proporcionar un camino claro y conciso para el diseño de la infraestructura de Active Directory, en un contexto propio de una OM. Serán tenidas en cuenta las mejores prácticas y experiencias, para ofrecer consideraciones y alternativas en cada punto del diseño.

Active Directory en la optimización de la Infraestructura según Microsoft.

Naturalmente, toda organización que no ha invertido en el desarrollo de estándares, aplicación de procedimientos de normalización, o implementación de herramientas/metodologías respaldadas en las mejores prácticas se caracteriza por

desarrollar procesos manuales y localizados. Así también posee un control central mínimo, políticas y estándares de TI inexistentes o no aplicados respecto a la seguridad, el respaldo, la administración e implementación de imágenes y otras prácticas de TI comunes. Este estado es el que el modelo de optimización de la infraestructura denomina estado o nivel “Básico”. Ver el modelo completo en el punto “Antecedentes y Marco Teórico” ya presentado. El siguiente nivel al cual se debería aspirar si se sigue el modelo mencionado es el “Estandarizado” (Microsoft, 2007). Así podríamos entender el proceso como pasar de un nivel a otro, luego de cumplir o “dar” diversos pasos. Es decir, se avanza en la optimización de la infraestructura. Para realizar este paso de niveles o evolución (Básico a Estandarizado) son necesarios cuatro pasos, y los detallamos a continuación:

- **Administración de identidad y acceso:** Implementación de un SD primario para autenticación y autorización
- **Administración de escritorios, dispositivos y servidores:** Automatización de la administración de actualizaciones de software e implementación de las mejores prácticas asociadas. Desarrollo de procesos de implementación basado en imágenes.
- **Seguridad y red**: Implementación de servicios de red (DNS y DHCP, por citar algunos) y despliegue de soluciones de protección de punto final administradas.
- **Protección y recuperación de datos:** Implementación de soluciones de respaldo/restauración para servidores críticos y administración de protección de datos (DPM) para servicios centralizados de respaldo y restauración.

No es el objetivo de este trabajo desarrollar todo o parte del modelo de optimización, sino tratar de identificar el par “contexto/tiempo” en el cual es saludable y óptimo comenzar el desarrollo de la implementación del Servicio de Directorio en la vida de las OMs. Así el inicio del proceso de optimización debe entenderse como la implementación del Servicio de Directorio central.

Escenario donde aplicar

La base del diseño se hará teniendo en cuenta que una OM operaría o abracaría modelos organizacionales ya descriptos. En este estudio abordaremos las

consideraciones que se refieren a la planificación y el diseño de los componentes necesarios para el éxito de la infraestructura del Servicio de Directorio de una organización mediana con un modelo similar a CDC con Intranet Organizacional, e incorporando posibles Unidades y/o Unidades Satélites.

Requisitos Lógicos para el Diseño Arquitectónico.

Antes de comenzar a desarrollar el flujo de trabajo para ir avanzando en el proceso de diseño del SD (Ilustración 9, más adelante), revisaremos los siguientes requisitos a niveles lógicos para el diseño de la arquitectura.

La facilidad que posee Active Directory para la delegación administrativa es una particularidad central a la hora de diseñar la estructura lógica del directorio. La administración específica de Unidades Organizacionales puede ser delegada para alcanzar la autonomía y/o el aislamiento de un servicio o datos. La delegación administrativa se emplea para resolver los requisitos de estructura legal, operacional, y de organización. Por ejemplo, la creación de cuentas de usuario se puede controlar centralizadamente; sin embargo, el acceso a archivos compartidos de personal puede ser controlado por un administrador en el departamento de personal. Esto último es una de las prácticas usadas y que mejor se adecuan a los requisitos de numerosas organizaciones del tipo medianas. Esto brinda agilidad y simpleza al diseño.

Proceso de diseño de Active Directory

Supuestos

Nos centraremos en hacer frente a decisiones de diseño importantes que enfrentan las OMs en la aplicación de Active Directory en un entorno operativo de Windows Server 2008.

En forma complementaria se mantendrá presente el objetivo de que el servicio se diseña en base a requerimientos, escenarios comunes, decisiones, actividades, opciones, tareas y resultados provenientes de OMs.

Recolección de Información

Entre los diversos tipos de información necesaria durante el proceso de planificación, la siguiente es requerida para el diseño de la infraestructura del SD:

- Necesaria para el diseño de las Unidades Organizativas de cada Dominio (A1).

  - El modelo administrativo utilizado actualmente en la organización. Esto se refiere a quien es responsable de gestionar los recursos informáticos en el ambiente. Otra forma de verlo sería preguntando "¿Quién hace qué a quién?"
  - Estrategias y requerimientos para el despliegue de las políticas de grupo.
- Necesaria para la ubicación de los controladores de dominio (B1).
  - El número de usuarios existentes por ubicación física. Ejemplo de lo anterior sería: en la oficina central, en cada unidad o unidad satélite).
  - El número de computadoras por ubicación física.
- Necesarios para crear el diseño del sitio (C1)
  - Mapa de distribución física de la organización.
  - Velocidades de conexión a la red y ancho de banda disponible entre localizaciones.
  - Direccionamiento IP de las subredes en cada ubicación física.
  - Dominios representados en cada ubicación física.
  - Cantidad de controladores de dominio (por dominio) en cada ubicación física.
- Necesaria para el diseño de los vínculos de sitios (C2): los objetivos de convergencia de replicación para los siguientes:
  - Esquema y Configuración.
  - Dominio
  - Catálogo Global
  - Particiones de Aplicación.

Decisiones involucradas

A continuación se abordarán las siguientes decisiones y/o actividades que se deben incluir en la preparación para la planificación del SD. Las siguientes trece medidas representan los elementos de diseño más importante para alcanzar un desarrollo bien planificado:

1. Determinar el número de bosques (**Paso 1**).
2. Determinar el número de dominios que incluirá cada bosque (**Paso 2**).

3. Asignar nombres de dominio (DNS) y los nombres NetBIOS para cada dominio (**Paso 3**).
4. Seleccione el dominio raíz para cada bosque (**Paso 4**).
5. Diseño de las unidades organizativas (OU) de la estructura de cada dominio (**Paso A1**).
6. Determinar la ubicación de los controladores de dominio para cada dominio (**Paso B1**).
7. Determinar el número de controladores de dominio (**Paso B2**).
8. Planificar la ubicación del servidor de Catálogo Global para cada uno de los Bosques (**Paso B3**).
9. Planificar la ubicación del Maestro de Operaciones Flexible Único (en Ingles: Flexible Single Master Operations –FSMO) para cada bosque y dominio (**Paso B4**).
10. Crear el diseño de Sitios (**Paso C1**).
11. Crear el diseño de los vínculos de Sitios (**Paso C2**).
12. Determinar el diseño de puentes de vínculos de Sitios (**Paso C3**).
13. Determinar la configuración de la instalación y el hardware necesario para los Controladores de Dominio. (**Paso D1**).

Flujo de la toma de Decisiones

La secuencia en la que se aconseja tomar las decisiones planteadas en el punto anterior es importante para el proceso de diseño. Aquí es bueno recordar que el camino crítico del proceso de diseño es el camino que ordena las decisiones en serie. Es decir que una tarea debe ser completada antes de que otra tarea comience (Microsoft, 2009).

El camino crítico para el diseño de Active Directory se presenta en el diagrama de flujo en la ilustración 9(más adelante). Se ha organizado el diagrama de manera que los pasos que deben ser llevados a cabo en una línea secuencial, han sido ubicados en la primera línea del diagrama. Algunos flujos del proceso se pueden realizar tanto en forma paralela o secuencialmente. Por ejemplo, los pasos A y B deben ser

completados, sin embargo, se puede realizar al mismo tiempo, A puede ser realizado antes de B, o viceversa.

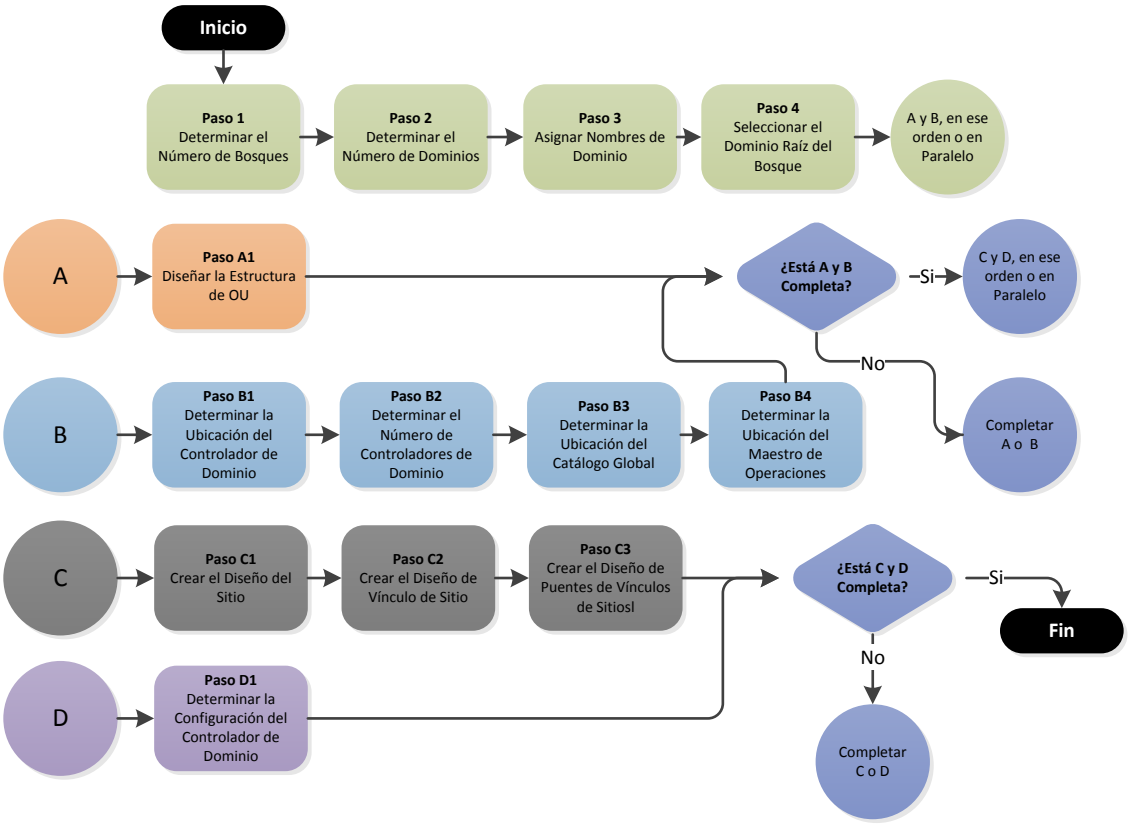

Ilustración 9. Ruta crítica y flujo del proceso para el diseño de Active Directory.

Desarrollo del proceso.

Paso 1: Determinar el Número de Bosques

Toda implementación de Active Directory deberá tener al menos un bosque. El primer paso en el diseño de Active Directory es determinar el número de bosques necesarios para cumplir los objetivos de la organización. Si se considera implementar más de un bosque, es necesario determinar en forma precisa el número total.

Es importante tomar la decisión correcta del número de bosques al comienzo de la fase de diseño. En la medida que la planificación avanza, los supuestos definidos sobre esta decisión harán más difícil los cambios en las configuraciones. Es considerablemente más difícil eliminar bosques ya establecidos que agregar bosques adicionales más adelante.

Opción 1: bosque único

Al considerar el diseño global de Active Directory, es conveniente comenzar con la implementación de un único bosque. Y a partir de esta consideración, dejar que del análisis de los requerimientos organizacionales se justifique la creación de bosques adicionales.

Para directorios extensos (numerosos bosques), la replicación comienza a ser más complicada. La información que involucran los dominios y bosques debe ser replicada.

Opción 2: varios bosques

Los requerimientos siguientes determinarán un diseño con varios bosques:

- **Varios esquemas.** Dentro del bosque se comparte un esquema común. Los conflictos entre aplicaciones en relación al esquema o por la administración de este puede introducir la necesidad de un bosque adicional.
- **Bosques de recursos.** Algunas organizaciones pueden requerir varios bosques por razones de aislamiento, pero con la necesidad de compartir un recurso común. Un bosque independiente puede ser creado para albergar los recursos compartidos, y relaciones de confianza entre los bosques pueden utilizarse para proporcionar la autenticación y la autorización de rutas de acceso. Un entorno de prueba puede ser creado como un bosque de recursos.

- **Desconfianza del administrador del árbol.** Algunas organizaciones tienen una estructura interna que incluye más de un equipo de TI. Cuando el equipo de cada una quiere controlar el bosque al tiempo que niega al otro grupo, o el control de personal, la aplicación de varios bosques es el medio para ese fin. Esta es una situación común cuando las empresas se fusionan, en determinados ámbitos de gobierno, o puede darse el caso en universidades.

- **Normas legales o motivos Geo-políticos.** Todos los dominios en un único bosque automáticamente definen una relación de confianza bidireccional (a nivel de Kerberos) para que datos y las aplicaciones se puede acceder fácilmente. Cuando se trabaja con diferentes países o regiones, los requisitos legales pueden dictar la separación de datos y aplicaciones. Varios bosques proporcionan esta separación.

La aplicación de varios bosques aumenta el costo de gestión del medio ambiente (infraestructura TI). Hardware y software adicional son necesarios para mantener y operar varios bosques, siendo también necesario personal adicional.

Si se requiere la interacción a través de bosques, las relaciones de confianza entre estos son necesarias y útiles.

Una consideración particular es que los Catálogos Globales no se replican a través de los límites del bosque. Para obtener una visión unificada en varios bosques, debe emplearse software adicional para la sincronización de directorios. La aplicación de estas tecnologías aumenta la carga administrativa al poseerse varios bosques.

Determinación del número de bosques

Al tomarse la decisión de definir varios bosques, se debe determinar el número exacto. Una forma de determinarlo es iterar a través de lo ya enunciado hasta que se satisfagan la totalidad de los requisitos organizacionales determinados por los objetivos generales. De este modo se determina el número de bosques necesarios.

A nivel de OMs es muy probable que se trabaje bajo el modelo de bosque único, lo anterior se basa en el número de recursos computacionales que posee una organización así clasificada.

Evaluación de las características

Complejidad		
Bosque único	Un único bosque es el punto de partida para una implementación de Active Directory, la complejidad no puede ser reducida.	Baja
Varios bosques	Dos o más bosques añaden incrementalmente mayor complejidad global al "medio ambiente" de TI.	Alta

Tabla 6. Análisis de Complejidad para el diseño de Bosques.

Costo		
Bosque único	Un bosque único es la opción de menor costo. Requiere menos hardware (el mínimo), software y apoyo administrativo.	Bajo
Varios bosques	Por cada bosque que se añade al diseño, se incrementa considerablemente el costo en hardware, software y tareas administrativas adicionales.	Alto

Tabla 7. Análisis de Costo para el diseño de Bosques.

Seguridad	
Bosque único	El bosque es el límite de seguridad, y el propietario de los bosques tiene acceso a todos los recursos dentro de este.
Varios bosques	El administrador de cada bosque posee responsabilidades únicas de seguridad. Esta división de responsabilidades entre administradores puede ser una solución granular de seguridad adecuada para ciertos entornos. Pensemos lo anterior desde un punto de vista de aislación.

Tabla 8. Análisis de Seguridad para el diseño de Bosques.

Validar con la organización

En esta etapa, además de evaluar las decisiones en base a los criterios relacionados con la TI, se deben tener en cuenta cómo afectan estas a la organización. Las siguientes preguntas pueden afectar a las decisiones de diseño de los bosques:

- ¿Existen planes de adquisición o fusión con otras organizaciones en un futuro próximo?

Si la empresa podría adquirir, ser absorbida o fusionarse en un futuro cercano, puede ser prudente replantear consideraciones del diseño del directorio con la otra

organización, en lugar de diseñar un directorio que podría desecharse una vez que la unificación se complete.

Si la acción es la adquisición de un nuevo negocio, las necesidades en torno a dicha adquisición deben ser consideradas durante la fase de diseño. Un ejemplo sería incluir los requisitos de la administración unificada y centralizada.

Si parte de una organización (unidad de negocio) va a ser cedida, un diseño de bosque separado podría hacer la transición más fácil y más simple.

Acciones y consideraciones

Para cada uno de los bosques en el ambiente TI, es importante considerar la sincronización del tiempo. AD es sensible del tiempo de los controladores de dominio, servidores y clientes que se sincronizan en cuestión de minutos unos de otros. De no existir tal sincronismo la autenticación Kerberos fallará. El tiempo es una de las variables consideradas para evaluar el estado de salud de una infraestructura de directorio. Active Directory se basa en el controlador de dominio que ejecuta el rol de "Controlador de Dominio Primario" (PDC, en inglés *Primary Domain Controller*), el cual define el tiempo maestro para todos los dominios en el bosque. Es decir todos sincronizan sus relojes contra él. Hay dos opciones para establecer el tiempo de ese controlador de dominio. Se puede configurar para sincronizarlo tanto desde una fuente interna o de una fuente externa a la organización. Un ejemplo de una fuente interna sería un dispositivo GPS. Y una fuente externa a la organización, podría ser un servidor de tiempo que está en Internet. Es conveniente emplear autenticación entre la fuente de tiempo y controlador de dominio para garantizar un tiempo de confianza.

No es recomendable emplear la actualización manual del tiempo en los recursos de los dominios. Como ya se mencionó, el entorno de Active Directory se basa fuertemente en el tiempo, y pueden presentarse graves problemas si no existe una adecuada sincronización del mismo.

Resumiendo, un bosque único es una buena recomendación para una OM. Es más simple de administrar, paseé menor costo de implementación, mantenimiento y soporte. Por características particulares de cada organización ya sean funcionales o legales entre otras, puede ser necesario el incremento del número de bosques. Si se presenta esta situación, es fundamental llevar a cabo las consideraciones que esto implica en cuanto al incremento de complejidad, carga administrativa y costos asociados.

Paso 2: Determinar el Número de Dominios

El segundo paso en el diseño de Active Directory para determinar el número de dominios que deberán cumplir los objetivos de la organización. Debido a que cada bosque es único y está separado “administrativamente” de los otros bosques, el número de dominios a definir en cada uno de los bosques puede ser analizado en forma separada en cada uno de ellos.

La adición o eliminación de un dominio después de que el diseño inicial se ha aplicado no siempre es sencillo. La migración de equipos, usuarios, datos y aplicaciones elevan la complejidad de realizar modificaciones en el número de dominios.

Opción 1: Caso de Dominio Único

En esta opción el diseño deberá tener al menos un dominio. Un modelo de dominio único tiene las siguientes ventajas y beneficios:

- Un único dominio es la opción menos costosa. Dominios adicionales aumentan los costos de hardware, software y gestión y operación.
- Un único dominio es la opción más simple de administrar.
- Un único dominio es más fácil de recuperar en caso de un desastre.

Opción 2: Caso de Múltiples Dominios

Los siguientes requisitos darán lugar a un diseño con varios dominios:

- En ambientes que constan de un número alto de usuarios u objetos de equipos, se deben realizar pruebas en laboratorio para garantizar que la carga de replicación de la información asociada a dichos objetos no abrume la topología de replicación para el dominio. Múltiples dominios pueden colaborar a reducir la carga global de replicación de un dominio.
- Si Active Directory tiene un gran número de atributos que cambian con frecuencia, puede ser útil llevar a cabo una división del “entorno”. De este modo se segmenta en varios dominios para controlar la replicación entre estos. Una práctica buena, dentro de las posibilidades, es realizar en un laboratorio esta división para determinar si varios dominios pueden reducir el tráfico de replicación de una manera significativa.

- Según el fabricante, el algoritmo de compresión utilizado para replicar los cambios del Servicio de Directorio a través de conexiones lentas es muy eficiente. Sin embargo, en caso de conexiones lentas podría causar problemas en la replicación. Un dominio adicional situado en el sitio remoto podría ayudar. Se debe tener en cuenta el punto anterior, ya que si hay muchos cambios o actualizaciones en los objetos del SD regularmente, puede requerir un análisis adicional.
- Un Servicio de Directorio ya existente, seguramente funciona con una versión anterior de NOS, y puede que sea necesario conservarlo por diversas razones. Por esto, quizás sea recomendable mantener ese servicio en su propio dominio, montando uno nuevo con todas las características de una nueva versión sin necesidad de mantener compatibilidades hacia atrás.

Al adoptar el modelo de tener varios dominios, el costo de la gestión del entorno se ve afectado de la siguiente manera:

- Personal TI adicional puede ser necesario para mantener los dominios. Cada uno de estos, quizás deberá tener su propio grupo de administradores.
- Un número mayor de dominios incrementa la complejidad de la administración. Esto también impacta en el nivel de especialización que deberá tener el personal asociado a este nuevo medio ambiente. Es decir, se trona en un medio ambiente más complejo.
- Hardware y software adicional debe ser adquirido para instanciar los dominios adicionales.

Determinar el número de Dominios

Definida la necesidad de múltiples dominios, el número exacto de dominios por cada bosque debe determinarse.

Evaluación de las características

Complejidad		
Dominio Único	Un directorio de un solo dominio es el ambiente menos complejo.	Baja
Varios Dominios	La complejidad aumenta con la adición de cada nuevo dominio. Sin embargo, cada dominio adicional no incrementa considerablemente la complejidad, sino impacta considerablemente en lo referente a costo asociado y capacidad de gestión.	Alta

Tabla 9. Análisis de Complejidad para el diseño de Dominios.

Costo		
Dominio Único	El costo de establecer y operar un único dominio es el más bajo posible.	Bajo
Varios Dominios	Los costos de preparación/inicialización aumentan con cada dominio adicional debido a los requisitos de instalación y configuración de cada controlador de cada dominio que se suma. Se incrementa también el costo de hardware y software para cada controlador de dominio extra.	Alto

Tabla 10. Análisis de Costos para el diseño de Dominios.

Validar con los objetivos organizacionales

Además de evaluar la decisión en este paso teniendo en cuenta los criterios relacionados con la TI, se deben considerar los objetivos organizacionales en este momento de diseño. Las siguientes preguntas se deben tener en cuenta para el diseño del dominio:

- **¿Existe una necesidad de separar un departamento o unidad de negocio debido a los requisitos legales?** Algunas empresas, y entornos universitarios, gubernamentales o militares requieren que algunos usuarios y equipos existan en un dominio independiente. Si esta política es necesaria, debe ser re-evaluado ya que un dominio en AD no es el límite de seguridad. Si la política es mantener el requisito de aislamiento, un bosque separado será requerido. Esto se entiende, ya que un administrador de la raíz del bosque, siempre tiene la posibilidad de tomar la posesión de cualquier recurso del mismo.

- **¿Existen diferentes unidades administrativas que deben ser autónomas?** En la mayoría de los casos, mediante la delegación en el nivel de unidad dentro de un único dominio puede proporcionar autonomía a las

unidades administrativas (concepto de Unidades Organizacionales). Sin embargo, por política, estructura organizacional, controles administrativos, y otros factores podrían generar la necesidad de dominios adicionales.

Consideraciones de diseño: Un diseño aconsejable en determinados escenarios, en especial donde el crecimiento es incremental y se valora la simplicidad, es el de trabajar con Dominios simples. Luego y dentro de estos Dominios modelar la organización mediante el empleo de Unidades Organizacionales. Esto aporta la aislación a nivel de unidades internas de la organización, y mantiene relativamente baja la complejidad de determinadas variables. En forma complementaria, una herramienta útil en etapas de diseño, es poder armar modelos o laboratorios mediante el empleo de servicios en la nube (*Cloud Services*). O a través del uso de hypervisores.

Resumiendo, un dominio único es la configuración predeterminada para cada bosque. Añadir dominios sólo cuando sea necesario para resolver los problemas técnicos y de negocio que no pueden ser resueltos dentro de un único dominio. Los dominios adicionales son más costosos ya que es necesario incrementar el hardware y el software necesarios para ejecutar los controladores de dominio en cada dominio. No hay que olvidar que el número de dominios debe ser determinado para cada bosque.

Una consideración adicional en relación a la virtualización: Es importante tener en cuenta que a la hora de emplear esta tecnología para la consolidación de servidores, toda la estructura de gestión del directorio es muy sensible al tiempo. Los algoritmos de seguridad empleados (como ejemplo Kerberos) emplean la variable tiempo como elemento fundamental de identificación y autentificación. Por lo cual el manejo de imágenes físicas o virtuales de un controlador de dominio debe ser manipulado con consideraciones muy especiales y perfectamente documentadas en lo referente a tiempo.

Paso 3: Asignar Nombres de Dominio

El tercer paso en el diseño de Active Directory es asignar nombres a cada uno de los dominios. Hay dos tipos de nombres para asignar: el nombre de dominio DNS y el nombre NetBIOS. Una de los avances más importantes en las versiones finales de la familia de servidores Windows 2008 fue la posibilidad de emplear de forma nativa DNS para la resolución de nombres. Lo anterior en lugar del Servicio de Nombres de Internet de Windows (WINS, en inglés *Windows Internet Naming Service*) de resolución de nombres NetBIOS, método que se utiliza en las versiones previas de los servidores Windows. Normalmente se requiere WINS para asegurar la compatibilidad hacia atrás. WINS se empleaba en la resolución de nombres locales (LAN) y se combinaba con DNS.

Tarea 1: Asignar Nombre de NetBIOS

La definición de nombres NetBIOS no posee una lista de opciones específicas. Sin embargo, hay consideraciones o consejos que son buenos considerar en el diseño del espacio de nombres.

Los nombres NetBIOS son los nombres que los usuarios ven más a menudo cuando se le pida un nombre de dominio de Windows. Cada dominio requiere que se le asigne un nombre NetBIOS. El nombre NetBIOS debe ser único en la red o la resolución de nombres dará como resultado ciertos conflictos.

El mismo nombre NetBIOS puede ser utilizado en diferentes organizaciones para representar a la misma entidad, por ejemplo, el nombre NetBIOS O*RG* puede ser utilizado a menudo como el nombre de la red interna de la organización. En este caso, si dos organizaciones se fusionan, y ambos han utilizado el nombre NetBIOS *ORG*, habrá un conflicto cuando se integran las dos redes.

Quizás sea bueno considerar para disminuir la posibilidad de conflictos en el uso de un nombre NetBIOS, emplear uno que sea único a través de las empresas, tales como *OESTEORG* para una compañía llamada “OESTE”. Utilice un nombre que sea único e independiente de los nombres regionales o de áreas existentes dentro de la organización.

Otra consideración es la de manejar nombres relativamente cortos, y con el mayor nivel de significancia posible. El abuso de siglas o iniciales puras, entorpece la posibilidad de entender un nombre asignado. Es bueno entender que los servicios de directorio actuales, son soluciones completamente transversales a la organización, por

lo cual sus interfaces serán empleadas por diversos niveles dentro de las mismas. Así, la definición de un espacio de nombre claro, cómodo de manejar y entender; ayuda considerablemente a la amigabilidad del medio ambiente de TI.

Tarea 2: Asignar el Nombre de DNS

Similar a lo planteado para nombre NetBIOS, la definición de nombres DNS no posee una lista de opciones específicas. Sin embargo, hay consideraciones necesarias de abordar en el diseño de este espacio de nombres.

Los nombres DNS de los dominios de Active Directory incluyen dos partes: un nombre de recurso y un nombre de red. Cuando son concatenadas estas partes se debe generan un nombre único para un recurso, no ambiguo. El nombre de recurso es el nombre de dominio de Active Directory.

En primer lugar, se debe determinar el nombre de la red. Una mejor práctica es que coincida con el nombre de dominio registrado en Internet para la organización. Si lo hace, se asegurará de que el nombre es único a través de Internet y no está en conflicto con otras empresas u organizaciones que tengan registrado el mismo nombre. Esto reduce el riesgo de conflictos de nombres en las fusiones y adquisiciones. Esto último es algo relativamente común en el ámbito privado.

En segundo lugar, seleccione el nombre de host para el dominio. El esquema de nombres por defecto hará que el nombre NetBIOS y DNS sea el mismo, tales como el nombre NetBIOS *OESTEORG* y el *nombre DNS* oesteorg*.com*. Para facilitar el seguimiento de los nombres DNS y NetBIOS en las interfaces de red; o para la resolución de problemas asociados con Active Directory o cuestiones relacionadas con él, es una buena idea mantener estos nombres. Sin embargo, no es indispensable.

Para garantizar la unicidad entre las empresas u organizaciones, no duplique los nombres de organizaciones existentes, registrada en Internet como nombres de dominio DNS. Es una buena práctica el registro de todos los nombres de dominio de nivel superior (también conocida como nombre de red), que están siendo utilizados, tanto interna como externamente, en InterNIC (en inglés *Internet Network Information Center*). Lo anterior con el fin de garantizar la unicidad de nombres de internet a nivel de DNS globales.

El despliegue y manejo de DNS conlleva una teoría subyacente bastante extensa y específica. Lo anterior escapa al alcance de este estudio, lo cual no le resta la importancia significativa que posee en relación a la infraestructura TI en general.

Validar con la organización

Además de evaluar las decisiones en este paso en contra de los criterios relacionados con lo referente a TI, las necesidades de la organización en lo referentes a objetivos y planes debe ser validado. Las siguientes preguntas deben ser contestadas ya que afectan a la toma de decisiones respecto al nombre de dominio:

- Se planea usar el actual nombre de dominio de Internet. ¿Existe algún grupo o aplicaciones que requieren un espacio de nombres DNS diferente, tal vez por razones de identidad? Será necesario definir un dominio separado para apoyar a un nombre DNS diferente dentro del bosque.
- ¿Está planeada alguna adquisición o fusión? Los cambios en la estructura empresarial pueden afectar a la estructura de nombres.

Resumiendo, los nombres de dominio deberían ser sencillos y deben ser coherentes con el espacio de nombres DNS de Internet. Tanto el nombre NetBIOS y el nombre DNS deben ser considerados teniendo en cuenta la coherencia, facilidad de gestión, y complejidad.

Una vez implementado, esta decisión es difícil de cambiar, ya que todos los equipos, aplicaciones y scripts necesitarían ser actualizados para representar el nuevo nombre. Además, los usuarios están relacionados con los nombres de dominio en el inicio de sesión y cuando se utilizan aplicaciones relacionadas con el dominio. Un cambio en el nombre de dominio podría ocasionar confusión y aparejar efectos perjudiciales en lo referente a identidades.

Importante: Es deseable que las ARs aporten las planillas de trabajo para ordenar la documentación y colaborar con el proceso de decisión para determinar el nombre de cada dominio, en cada bosque. Ejemplos de estas planillas se adjuntan más adelante en el Anexo.

Paso 4: Seleccionar el Dominio Raíz del Bosque

El primer dominio que se despliega en un bosque de Active Directory se denomina el dominio raíz del bosque. Este dominio sigue siendo el dominio raíz del bosque durante todo el ciclo de vida de la implementación de Active Directory. No es posible cambiar esto, sin la redistribución completa del bosque.

El dominio raíz del bosque contiene los grupos Administradores de la Organización y Administradores del Esquema. Estos grupos de administradores se utilizan para gestionar las operaciones a nivel de bosque, tales como la adición y la eliminación de dominios y futuros cambios en el esquema.

Un dominio existente en el diseño puede ser seleccionado como la raíz del bosque, o como raíz dedicada del bosque. Estas dos opciones las explicaremos un poco más adelante (Opción 2). Una vez que el dominio raíz del bosque se ha establecido, no puede ser cambiado sin la reconstrucción del bosque.

Opción 1: Utilizar un Dominio Planificado

Cuando el diseño de dominios de un bosque indica la existencia de un único dominio, entonces este único dominio es del dominio raíz del bosque. Este dominio almacena a todos los usuarios, grupos, equipos, y los grupos de la raíz del bosque.

Si existen varios dominios en el diseño, uno de los dominios puede ser seleccionado para ser el dominio raíz del bosque, además de la gestión de los usuarios y recursos del dominio. El dominio seleccionado define el espacio de nombres del bosque y tendrá que ser el primer dominio desplegado en el entorno. A pesar de que también gestionará usuarios y recursos, siempre mantendrá su condición única como el dominio que contiene los grupos Administradores de la Organización y Administradores del Esquema.

Opción 2: Utilizar un Dominio como Raíz Dedicada del Bosque

Un dominio como raíz dedicada del bosque, también conocido como raíz de bosque vacía, puede ser añadido a la estructura de dominios existente específicamente para gestionar las funciones a nivel de bosque. Cuando se selecciona, este dominio no contiene ninguna cuenta de usuario u otros recursos, salvo las cuentas de administración del servicio para el dominio raíz del bosque. Este tampoco representa ninguna región en la estructura de dominio. Todos los dominios se transformarán en hijos de este dominio jerárquicamente hablando.

El diseño de raíz de bosque dedicada generalmente es elegido por las siguientes razones:

- Separación funcional de los administradores de servicios forestales de los administradores de servicios de dominio.
- Protección de los cambios operativos en otros dominios.
- Sirve como una raíz neutral para que ninguna región parezca estar subordinada a otra región.

También es muy importante considerar que esta opción de diseño, raíz dedicada de un bosque, presenta las siguientes desventajas:

- Una sobrecarga de trabajo adicional aparece en el seguimiento y mantenimiento de los controladores de dominio asociados a la raíz. Los controladores de dominio que definen la raíz del bosque dedicada deben estar disponibles a fin de permitir a los usuarios obtener acceso a los recursos de otros dominios.
- Saltos adicionales se insertan en las rutas de confianza a los controladores de dominio a fin de permitir a los usuarios obtener acceso a los recursos en otros dominios, salvo que se apliquen relaciones de confianzas directas.

Cabe señalar, sin embargo, que las funciones a nivel de bosques no están protegidas de un administrador con malas intenciones quien puede manipular la base de datos de Active Directory de tal manera que comprometa la integridad y seguridad del directorio. Esto significa que mientras una raíz del bosque vacío puede separar grupos funcionales administrativos, no concede ninguna garantía adicional en el ámbito del bosque de los administradores deshonestos. Aquí es bueno plantear que el límite de seguridad es el bosque. Es decir la mínima unidad administrativa en concepto de seguridad es el bosque. Un administrador de un bosque puede tomar posesión de cualquier recurso dentro del mismo.

Evaluación de las características

Costo		
Utilizar un Dominio Planificado	No se generan costos adicionales al emplear un dominio ya planificado como raíz del bosque.	Bajo
Emplear un dominio raíz vacío	El definir un dominio raíz vacío como raíz del bosque (nuevo dominio) conlleva la necesidad de emplear hardware adicional y licenciar software para las computadoras que definen el dominio. En forma adicional será necesario asegurar su disponibilidad.	Alto

Tabla 11. Análisis de Costo de la selección del tipo de dominio raíz.

Validar con los objetivos organizacionales

Además de los criterios relacionados con las TI, es importante contemplar los objetivos y necesidades de la organización en esta etapa del diseño. Aquí, es importante ampliar la visión y el alcance que el diseñador posee de la organización. Es común que ciertos proyectos tecnológicos dentro de las organizaciones comiencen en áreas conocidas y bien definidas. Por la naturaleza transversal que posee la tecnología que involucra el Servicio de Directorio, es aconsejable que se tome el recaudo de analizar seriamente el alcance que puede tener a futuro el crecimiento del directorio. En organizaciones privadas es común que se presenten situaciones de compras y/o fusiones, lo cual seguramente afectará la colocación de la raíz del bosque. En organizaciones públicas o Universidades se suele presenta la necesidad de expansión de la cobertura del servicio. Inicialmente se comienza implementando en un área particular de la organización, y posteriormente surge la necesidad de expandirse al resto de la misma.

Por lo descripto, es una buena práctica de diseño, llevar a cabo un análisis profundo de la realidad actual y futura de la organización. Así, poder tener fundamentos para tomar decisiones con cierta previsibilidad.

Resumiendo, en este punto se ha determinado la identidad del dominio raíz del bosque. Las opciones posible son elegir un dominio ya planificado, o se ha decido añadir un nuevo dominio como raíz del bosque.

Paso A1: Diseñar la Estructura de Unidades Organizativas

Los objetos incluidos en el directorio se organizan mediante el uso de las unidades organizativas (en adelante, UO). El diseño de las unidades organizativas se basa en dos aspectos principales: la delegación de la administración de los objetos del directorio y la aplicación de Objetos de Políticas de Grupo (en inglés *Group Policy Objects, GPO*). Fundamentalmente, como una de las premisas de diseño las unidades organizativas deben reflejar la forma en que se gestionan los objetos dentro del dominio.

Cambiar el diseño de las unidades organizativas una vez definidas no es difícil. Pero lo anterior acarrea ciertas precauciones, ya que las listas de control de acceso deben ser cuidadosamente manipuladas. Una vez que la delegación y las políticas de grupo se han establecido, el rediseño de las unidades organizativas llevará algún tiempo, en especial a las cuales se les han aplicado las configuraciones.

Dado que las unidades organizativas pueden usarse para el doble papel de la delegación de la administración y la aplicación de la directiva de grupo, será necesario pasar por el proceso de diseño de las unidades organizativas dos veces: una basándose en la delegación y luego una segunda vez con un mirada hacia la implementación de Políticas de Grupo.

Tarea 1: Diseñar las Unidades Organizativas para la delegación de la administración

Las unidades organizativas pueden ser empleadas para delegar la administración de objetos, como usuarios o equipos, o de un grupo designado. Aunque es posible delegar permisos en forma individual, es una buena práctica emplear el concepto de grupo de usuarios. Al producirse cambios en la organización, es más simple actualizar la pertenencia a los grupos de administración que actualizar los permisos asignados a cada usuario sobre los objetos en el directorio. Esto es esencialmente el concepto de administración basada en grupos.

El empleo de unidades organizativas para la delegación de la administración implica las siguientes actividades:

- Identificar o crear grupos con derechos administrativos a los cuales se les va a delegar parte de la administración.

- Ubicar individuos o grupos a los cuales se les van a delegar los derechos en la unidad organizativa. Crear las unidades organizativas sobre las cuales los grupos administrativos tendrán autoridad.
- Asignar los derechos del objeto que se delegue en el grupo administrativo, dentro de cada unidad organizativa.
- Crear /ubicar los objetos a ser controlados dentro de la unidad organizativa.

Al identificar los grupos a los cuales se les delegarán las tareas administrativas, hay que ser específico respecto a la cantidad mínima de control que se delegará. Como ejemplo simple podemos citar que si un grupo necesita sólo la capacidad de actualizar la información referida a los teléfonos de los usuarios, no se le debe conceder el control total.

Tarea 2: Diseñar la configuración de Unidad Organizacional para la aplicación de directivas de grupo.

Las Unidades Organizacionales (OU, en inglés *Organizacional Unit*) pueden ser creadas para aplicar directivas de grupo a un subconjunto específico de equipos o usuarios. Por defecto, todos los objetos en una unidad recibirá la configuración contenida en un GPO aplicados a dicha unidad.

Con el diseño completado de la OU desde una perspectiva de delegación (u operación), el siguiente paso es revisar el diseño de la OU para tener en cuenta cualquier circunstancia única de que la configuración de directiva de grupo pueden introducir. Por ejemplo, desde una perspectiva de la delegación, una unidad organizativa, podría establecerse llamándola "estaciones de trabajo" para delegar permisos para administrar todas las estaciones de trabajo. Cuando se aplica la política de grupo, puede haber una necesidad de una OU para estaciones de trabajo de escritorio y una OU para estaciones de trabajo móviles para reflejar las diferentes necesidades para equipos de escritorios y portátiles. En este caso, se pueden crear dos OUs como sub-unidades organizativas dependiendo de la OU “estaciones de trabajo”. O sustituir la OU “estaciones de trabajo” por estas dos unidades individuales.

Identifique los grupos de usuarios o máquinas a las que un GPO tiene que ser aplicado. Luego, examine el diseño actual de la OU para el dominio. Re-use las unidades organizativas existentes, si es posible y solo cree unidades organizativas nuevas si es necesario. Si crea unidades organizacionales para apoyar a los GPOs, asegúrese de revisar la delegación de los objetos creados en la tarea anterior para

garantizar que el modelo de administración y operación de los mismos esté actualizado.

Hay muchas opciones para definir el filtrado y el enfoque de la aplicación de las directivas de grupo. El filtrado de seguridad, el filtrado mediante WMI, y las preferencias de las políticas de grupo se pueden usar para definir el alcance de cuales objetos recibirán las GPO. Se deben utilizar estas técnicas, como último recurso, en lugar de emplear la aplicación y precedencia por defecto de Directivas de grupo. El filtrado de seguridad mediante directiva de grupo es muy difícil de gestionar y solucionar, pudiendo causar una ligera degradación del rendimiento de los inicios de sesión de los clientes.

Resumiendo, la estructura de unidad organizativa debe ser definida en la etapa de diseño para cada uno de los dominios. Al final de esta decisión, el diseño de la OU debería haber identificado lo siguiente:

- Unidades organizativas que van a ser creadas, sobre la base de uno de los dos criterios de diseño: la delegación de la administración o aplicación de la directiva de grupo.
- Qué objetos tienen que estar ubicados en cada unidad organizativa.
- Grupos de Administración/Delegación que se creen y se asignan a las unidades organizativas.
- Derechos de objetos que se concederán a cada grupo en cada unidad organizativa.
- Qué objetos de políticas de grupo se deben crear y a que unidades organizativas deben ser vinculados.

Paso B1: Determinar la Ubicación del Controlador de Dominio

Típicamente, una topología de la red tendrá determinados lugares físicos (recintos grandes o edificios de oficinas y centros de datos) que se consideran “centros” o concentradores (en inglés *hub*). En estos hay concentraciones de usuarios, equipos o conectividad de red. A su vez pueden conectarse a cierto número de localizaciones tipo satélites más pequeñas, como sucursales u oficinas reducidas. Estas sucursales o unidades reciben servicios de red o recursos de computación, pero no suelen prestar servicios a otras oficinas satélites. A forma de resumen, podemos hablar del modelo organizacional de CDC, con la extensión de ser necesaria de ampliar el modelo, para cubrir el concepto de Unidad o Unidad Satelital.

En este paso, se deberá decidir que recursos de controlador de dominio será colocado para cada dominio en cada bosque. El paso B2 definirá cuantos controladores de dominio se colocarán en cada lugar para cada dominio.

Con el fin de reducir costos y complejidad y aumentar la capacidad de administración, es conveniente colocar los controladores de dominio en pocos lugares como sea posible y en el que tendrán la mejor utilización y el mejor impacto para la organización.

Una consideración adicional, y bastante lógica, es que cada dominio debe tener un controlador de dominio en al menos dos ubicaciones geográficamente dispersas para permitir la disponibilidad del servicio. Lo anterior es para prevenir que en alguno de los dos lugares suceda un evento no esperado que afecte al Servicio de Directorio.

Todos los controladores de dominio tienen que estar físicamente asegurados. Si no se puede asegurar la seguridad física en un lugar, un controlador de dominio full no se debe colocar en ese lugar, sin embargo, se podría implementar un controlador de dominio de solo lectura en un lugar donde la seguridad física es una preocupación.

La decisión respecto al lugar donde alojar el controlador de dominio puede cambiar de forma relativamente sencilla en cualquier momento.

Tarea 1: Localización en los centros (HUBs)

Los centros prestan servicios de red y de computación a muchos usuarios dentro de la organización. Estos centros pueden proporcionar estos recursos a los usuarios, así como a una o más unidades satélites.

Al ser estos centros de distribución un punto central, poseen un fuerte impacto en lo referido al valor estratégico de la distribución.

Un centro puede ser el punto de agregación para las unidades satélites. Es menos costoso que el centro aloje al controlador de dominio, que tener un controlador de dominio emplazado en cada ubicación individual.

Determine qué centros de localización recibirán los controladores de dominio para cada dominio, y comience a documentarlo.

Tarea 2: Localización en las unidades satélites

Las unidades satélites están conectadas a la red organizacional a través de los centros. En la mayoría de los casos, una localización satélite tiene menos usuarios y computadoras que un centro. Los clientes ubicados en los satélites pueden utilizar los recursos a nivel local, los recursos en el centro, o puede utilizar el centro para acceder a recursos ubicados en otras partes de la red organizacional. Ciertas consideraciones pueden indicar la necesidad de implementar un controlador de dominio en un sitio satélite.

Los controladores de dominio necesitan ser administrados. Asegúrese que en los lugares que emplace los controladores de dominio estos puedan ser administrados localmente o de forma remota mediante el uso de conexiones seguras.

La comunicación con un controlador de dominio es esencial para la autenticación del acceso a recursos de red. Por lo tanto, si el vínculo WAN/MAN entre la oficina satélite y el centro no es confiable y no rentable económicamente la actualización, considere colocar un controlador de dominio en la oficina satélite para efectuar localmente las autentificaciones de los clientes.

Otro factor para considerar en la ubicación del controlador de dominio en una oficina satélite es si el ancho de banda del enlace WAN/MAN es suficiente tanto para tráfico rutinario de red como para la autenticación. En ciertos casos, el ancho de banda disponible entre la oficina satélite y el centro es empleado en su totalidad por las aplicaciones o servicios. Por lo cual no hay margen para el tráfico asociado a la autenticación. En este caso, un controlador de dominio local en la oficina satélite podría ser necesario.

Otra consideración para colocar un controlador de dominio en una oficina satélite es dar cabida a los servicios y recursos que podría residir en la oficina satélite.

Servicios tales como DNS y Sistema de archivos distribuido (DFS), así como los recursos como el correo y bases de datos, podría beneficiarse de tener un controlador de dominio en la misma subred en lugar de tener que cruzar un enlace WAN/MAN para la autenticación y la gestión del directorio.

La autonomía de los sitios es a veces una razón para colocar los controladores de dominio en los mismos. Por ejemplo, si una empresa tiene una planta de fabricación en una ubicación remota y los equipos de la línea de producción requieren autenticación para operar, es aconsejable colocar un controlador de dominio en el sitio. Esto permitirá seguir fabricando independientemente de la disponibilidad del vínculo WAN/MAN.

Determinar qué unidades satélites serán las sedes donde se alojarán los controladores de dominio para el cada dominio, y luego registrar las decisiones.

A modo de resumen, ubique controladores de dominio en el centro y en las oficinas satélites donde sea apropiado. La mayoría de los Centros requieren uno o más controladores de dominio. Las oficinas satélites pueden requerir un controlador de dominio en función de características del enlace WAN/MAN, el número de clientes, y los recursos disponibles.

Es necesario repetir este proceso de decisión para cada dominio en cada bosque.

Paso B2: Determinar el Número de Controladores de Dominio

En el paso B1 vimos la necesidad de determinar la ubicación física de los controladores de dominio. Analizaremos la decisión relacionada de determinar el número de controladores de dominio para cada ubicación.

Hay diversos factores para decidir cuantos controladores de dominio se deben implementar para cada dominio. Las decisiones se basan en el rendimiento de las autenticaciones, el acceso a los recursos, la replicación, y el costo.

Tarea 1: Determinar el número de controladores de dominio

Se debe definir el número mínimo de controladores de dominio para cada dominio en cada localización identificada en el Paso B1. La siguiente tabla describe el número mínimo de controladores de dominio necesarios, tomando como referencia el número de usuarios.

Usuario por cada dominio en un sitio	Número mínimo de controladores de dominio necesarios por cada dominio en un sitio
001 - 499	Uno – Procesador simple
500 - 999	Uno - Procesador dual
1.000 - 2.999	Dos - Procesador dual
3.000 – 10.000	Dos – Procesador Cuádruple

Tabla 12. Número mínimo de controladores de dominio.

Para cargas de trabajo en un sitio de más de 10.000 usuarios, se deben realizar pruebas adicionales para determinar las necesidades de hardware.

Si sólo existe un controlador de dominio en cada localización, se debe prever la posibilidad de que cada uno de los sitios, mediante un vínculo WAN/MAN pueda comunicarse con un controlador de dominio para efectuar la autenticación y el acceso a los recursos en el caso de que falle el controlador de dominio local.

De darse el caso de que una implementación superara los 15 controladores de dominio en un dominio particular, se debe considerar la necesidad de implementar un controlador de dominio adicional al sitio. Hay que tener en cuenta que la replicación de la base de datos del directorio se efectúa entre los controladores de dominio, independientemente de los sitios. Si bien estas consideraciones son importantes, de

cumplirse, estaríamos frente a una organización no del tipo mediana. Por lo cual excede al alcance propuesto en el presente estudio. Lo importante a tener en cuenta es la necesidad y la relevancia que implica la replicación de un Servicio de Directorio entre sus controladores.

Es importante considerar y tener debidamente documentado todas las aplicaciones que se basan en datos de Active Directory. Algunas aplicaciones, como puede ser Exchange Server o un servicio de mensajería, suelen requieren controladores de dominio adicionales para funcionar correctamente. Es importante evaluar la necesidad de implementar controladores de dominio adicionales considerando cargas previstas y los requisitos de las aplicaciones.

Tarea 2: Determinar el tipo de controlador de dominio que se ubicará en un sitio

Es necesario determinar qué tipo de controlador de dominio será implementado en cada caso. Si se tratará de un controlador de dominio de escritura o de solo lectura (RODC, en inglés R*ead Only Domain Controller)*. Se deberá efectuar el análisis de lo anterior para cada uno de los controladores de dominio que se decidan implementar en el Servicio de Directorio. Un controlador de dominio completo o de escritura, sólo debe colocarse en lugares donde la seguridad física del mismo puede ser garantizada.

La razón principal para usar un RODC es para lugares con la seguridad física deficiente. Ya que no es posible realizar cambio alguno en un RODC y luego replicarlo hacia un DC de escritura. Un RODC requiere acceso a un DC de escritura para fines de autenticación. De forma predeterminada, ningún hashes de contraseña se replica en un RODC. El RODC remite la solicitud de inicio de sesión a un controlador de dominio de escritura. Es posible configurar el entorno para que el controlador de dominio completo (o de escritura) replique el hash solicitado al RODC para almacenar en caché local. Es bueno saber que de configurarse lo anterior y el RODC es comprometido desde un punto de vista de seguridad, sólo es necesario blanquear los hashes de réplica en el RODC.

La funcionalidad proporcionada por el RODC puede verse afectada si el vínculo WAN es lento o un controlador de dominio completo jerárquico no está disponible para atender las solicitudes del RODC.

Es importante determinar qué controladores de dominio serán de escritura y cuáles de solo lectura, y luego registrarlo en las planillas de trabajo.

En resumen, es importantísimo entender que es necesario un mínimo de dos controladores de dominio para ofrecer disponibilidad en un dominio. Sobre la base de los requisitos organizacionales descriptos anteriormente, los controladores de dominio se pueden colocar en lugares físicos específicos para realizar la autenticación local. Controladores de dominio adicionales pueden ser necesarios en base a necesidades de autenticación de usuarios y requisitos de las aplicaciones. El uso de servidores tipo RODC puede aumentar considerablemente la seguridad y también el rendimiento. El costo de la adición de estos servidores en los escenarios correctos debe ser considerado.

La decisión de añadir o quitar controladores de dominio puede cambiar en cualquier momento.

Paso B3: Determinar la Ubicación del Catálogo Global

Los servicios de Catálogo Global facilitan la búsqueda de información a todos los dominios del bosque, especialmente a los dominios fuera del dominio actual. El catálogo es un subconjunto de la información de cada dominio que se replican en cada servidor de catálogo global del bosque. Aplicaciones tales como Exchange Server dependen en gran medida del catálogo global respecto a información pertinente. El catálogo global también se utiliza durante el proceso de inicio de sesión para reconocer los miembros del grupo universal.

Todos los servicios de catálogo global residen físicamente en uno o más controladores de dominio. No hay forma de separar la funcionalidad de catálogo global de la de un controlador de dominio.

La decisión a tomar es respecto a que controladores de dominio en el bosque serán los que alojen los servicios de catálogo global.

Tarea 1: Determinar la localización del Catálogo Global

Si un bosque está formado por sólo un dominio, entonces todos los controladores de dominio deben ser configurados como servidores de catálogo global. El subconjunto de los datos que se replican en todos los catálogos globales se realiza a través del proceso normal de réplica de dominio. No habrá entonces requisitos adicionales para el uso de espacio en disco, uso de CPU, o el tráfico de replicación. Esta es sin dudas una situación ideal desde el punto de vista de simplicidad de la administración. Así, desde el punto de vista de una Organización Mediana

Si un bosque contiene varios dominios, normalmente cada controlador de dominio no debe ser un servidor de catálogo global, debido al aumento de las necesidades de almacenamiento y la sobrecarga de replicación adicional que conlleva.

En un entorno de un bosque con múltiples dominios, un subconjunto de los controladores de dominio se configura para desempeñar el rol de servidores de catálogo global. Debido a que todos los catálogos globales replican sólo un subconjunto de todos los objetos de cada dominio, la ubicación del catálogo global debe ser cuidadosamente considerada en relación a la sobrecarga de mayor ancho de banda introducida por el tráfico adicional. Además, hay un aumento de requisitos de hardware para el almacenamiento de datos de catálogo global. La ilustración 10 muestra el árbol de flujo de decisión para decidir dónde colocar los catálogos globales en el medio ambiente.

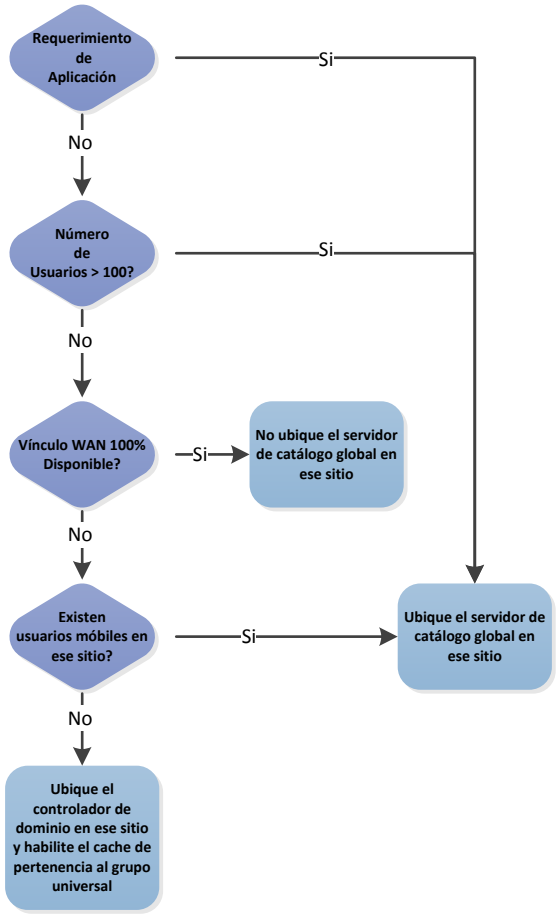

Ilustración 10. Árbol del flujo de decisión para la ubicación de los servidores de catálogo global en el medio ambiente.

¿Existen aplicaciones que necesitan un servidor de catálogo global ejecutando localmente?

Algunas aplicaciones, tales como Exchange Server, Microsoft Message Queue Server (MSMQ) y aplicaciones que utilizan COM distribuido (DCOM), dependen en gran medida de los servidores de catálogo global. Estas aplicaciones tienden a funcionar mejor cuando tienen un catálogo global disponible a nivel local para mejorar los tiempos de consulta/respuesta.

Puede haber algunas restricciones de uso alrededor del empleo de un RODC como catálogo global. A continuación se sita un ejemplo de un servicio como Exchange Server, el cual es la plataforma de mensajería de Microsoft, la cual no es compatible con los catálogos globales que se ejecutan en un RODC, sin embargo, los clientes de correo como Outlook y los clientes de mensajería de colaboración pueden utilizar un RODC con el rol de catálogo para la búsqueda en las libreta de direcciones.

Si bien, este ejemplo es algo particular, sirve para visualizar o contextualizar la integración del Servicio de Directorio con aplicaciones y servicios puntuales.

¿Es mayor a 100 el número de usuarios locales?

Se deberían ubicar servidores de catálogo global en cualquier lugar que tiene más de 100 usuarios, a fin de reducir el tráfico sobre vínculos WAN/MAN, evitando pérdida de productividad en caso de fallos de los enlace. Si bien esto es lo especificado, existe alguna flexibilidad. Es posible colocar un mayor número de estaciones de trabajo. Lo anterior es factible, dependiendo del uso intensivo que se le dé al Servicio de Directorio. Es decir, la cantidad de aplicaciones y procesos que accedan y consulten los catálogos.

Fiabilidad del enlace WAN/MAN

Considere colocar un servidor de catálogo global en un lugar en el que el vínculo WAN no es lo suficientemente fiable para garantizar la autenticación de usuario, o bien configurar el almacenamiento en caché de la pertenencia al grupo universal.

¿Pueden varios usuarios itinerantes trabajar localmente?

Los usuarios móviles necesitan comunicarse con un servidor de catálogo global cada vez que inicien sesión por primera vez independientemente del sitio. Por lo tanto, un servidor de catálogo global debería ser colocado en sitios que involucren muchos usuarios itinerantes. Es común que los inicios de sesión sobre el enlace WAN causen un aumento considerable del tráfico WAN, lo que conlleva a la degradación del rendimiento y pérdida de producción.

¿Es suficiente el cache local para los miembros de los grupos universales?

Contar con almacenamiento en memoria cache local de los miembros del grupo universal es una opción para los sitios que incluyen menos de 100 usuarios y no poseen numerosos usuarios móviles o aplicaciones que requieren un servidor de catálogo global.

Cuando un usuario inicia sesión en la red, el servidor de catálogo global es contactado para consultar la pertenencia de este a grupos universales. A través de vínculos lentos, este proceso puede tomar una cantidad significativa de tiempo o, en el caso de fallar la conexión con el servidor de catálogo global, puede resultar en la negación en el proceso de inicio de sesión. La implementación en cache local del almacenamiento de grupos universales se puede utilizar para abordar este problema.

¿Cuantos catálogos globales son necesarios?

Una vez que se ha determinado que los servidores de catálogo global son necesarios en una ubicación, la siguiente pregunta es cuántos son necesarios. En la mayoría de los casos, uno o dos servidores de catálogo global serán suficientes en cada lugar. Requisitos de algunas aplicaciones tales como los servidores de mensajería (Exchange Server), puede aumentar el número de servidores de catálogo global necesarios. Si bien lo anterior es al necesario, es un requerimiento particular para implementaciones específicas, en las que se piense trabajar con servicio de mensajería.

Es fundamental registrar que controladores de dominio se configuran como catálogos globales.

Validar con los objetivos organizacionales

Además de evaluar las decisiones vistas en este paso en contra de los criterios relacionados con las TI, el efecto de la decisión sobre los objetivos organizacionales también debe ser tenido en cuenta. La siguiente pregunta puede afectar a la decisión de la ubicación del catálogo global:

- **¿Hay usuarios que viajan frecuentemente a las sucursales o unidades y que requieren servicios de inicio de sesión y de servicios de directorio en esos sitios?** Un servidor de catálogo global puede ayudar o solucionar los requerimientos de los usuarios móviles respecto a la necesidad de solicitar servicios locales.

En resumen, configurar los controladores de dominio como servidores de catálogo global sólo cuando hay razones técnicas para hacerlo. Se pueden hacer excepciones cuando una población de usuarios itinerantes requiere servicios de alto rendimiento de catálogo global en sitios fuera de los dominios de los usuarios.

Mantenga el número de servidores de catálogo global a un mínimo para reducir los costos, la gestión, y la complejidad de la configuración y el mantenimiento.

El diseño de los servidores de catálogo global se debe repetir para cada uno de los bosques.

Paso B4: Determinar la Ubicación del Rol de Maestro de Operaciones

El siguiente paso es decidir la ubicación de las funciones de maestro de operaciones del bosque y de cada dominio (también conocido como FSMO por sus siglas en ingles *flexible single master operations*). Aunque cada controlador de dominio de Active Directory puede autenticar cuentas y escribir en el directorio de base de datos, algunas funciones están dedicadas a un solo controlador de dominio. Las funciones de FSMO existen en un controlador de dominio designado, el cual controla funciones específicas de dominio y de bosque.

Existen tres funciones FSMO para cada dominio:

- **Maestro de Operación de Emulador de PDC.** Esta función procesa todas las solicitudes de replicación provenientes de Controladores de Reserva de Windows NT 4.0 (BDC) y procesa todas las actualizaciones de contraseñas para clientes que no ejecutan el cliente de Active Directory. Este es también el controlador de dominio predeterminado que se utiliza para la actualización de Directivas de Grupo.

- **Maestro de Operación de identificadores relativos (RID).** Cuando se crea un nuevo objeto en el directorio, el Controlador de Dominio correspondiente crea una entidad de seguridad (en inglés conocida como *security principal*), que representa al objeto. A esta entidad le asigna un identificador único de seguridad SID (en inglés *unique Security Identifier*). El SID consiste en un SID a nivel de dominio, que es igual para todas las entidades de seguridad creadas en el dominio, y un identificador relativo (RID, en inglés *relative identifier*), el cual es único para cada entidad creada en el dominio. El Maestro RID asigna bloques de RIDs a cada Controlador de Dominio dentro del Dominio. Luego el Controlador de Dominio asigna el RID a los objetos que se crean, desde este bloque.

- **Maestro de Operación de infraestructura.** Este rol mantiene una lista de las entidades de seguridad de otros dominios que tienen pertenencia en grupos dentro del dominio del maestro de operaciones. Cuando los objetos se mueven de un dominio a otro, el Maestro de Infraestructura actualiza las referencias al objeto en ese dominio y la referencia al objeto en el otro dominio. La referencia del objeto contiene el identificador único global (GUID, en inglés *Object Globally Unique Identifier*), el Nombre Distintivo o completo (DN, en inglés *Distinguished Name*) y el SID. El Servicio de Directorio actualiza

periódicamente el DN y el SID, en la referencia al objeto para reflejar los cambios realizados en el objeto real, por ejemplo, movimientos en y entre dominios o la eliminación de este.

Es bueno recordar que cada dominio en el bosque tiene su propio Emulador PDC, Maestro RID y Maestro de Infraestructura.

En forma complementaria hay dos funciones de maestro para cada uno de los bosques:

- **Maestro de Operación del Esquema.** Esta función permite cambios en el esquema, controlando todas las actualizaciones al mismo. El esquema contiene la definición de las clases de objetos y atributos que se utilizan para crear todos los objetos dentro del Servicio de Directorio como son usuarios, computadoras e impresoras.
- **Maestro de Operación de nombres de dominio.** Este rol controla la adición o el retiro de dominios en el bosque. Cuando se agrega un nuevo dominio al bosque, solamente el DC que tenga el rol de maestro de nombres de dominio podrá agregar el nuevo dominio. Existe solamente un Maestro de Esquema y un Maestro de Nombres de Dominio por Bosque.

Como pauta general de simplicidad, es aconsejable mantener los maestros distribuidos en pocos controladores de dominio dentro de las posibilidades, con el fin de simplificar el seguimiento y la operación. Si la carga en el maestro de operaciones justifica un cambio, colocar el RID y el rol de PDC en los controladores de dominio distintos dentro del mismo sitio. Los controladores de dominio deben ser asociados directos de replicación.

En general, el maestro de infraestructura no debe ser colocado en un servidor de catálogo global. Si un maestro de infraestructura se encuentra en un servidor de catálogo global, no se identifican correctamente las entidades de seguridad obsoletas de otros dominios. La excepción es en los ámbitos en los que todos los controladores de dominio son servidores de catálogo global o en un bosque de dominio único. En estos casos, el maestro de infraestructura posee toda la información que necesita.

El maestro de esquema y el maestro de nombre de dominio rara vez se utilizan y no deben minuciosamente controlados; es aconsejable mantenerlos juntos en el

mismo controlador de dominio que aloja el catálogo global. Algunas operaciones, como crear dominios secundarios, utilizan el maestro de nombres de dominio y fallará si el rol no está en un servidor de catálogo global.

Coloque estos controladores de dominio en el lugar donde se ubiquen la mayoría de los usuarios de ese dominio y que disponga de un servicio de red altamente fiable. La ubicación del Maestro de Operaciones puede ser modificada fácilmente.

Todas las funciones FSMO se deben colocar en los controladores de dominio que están disponibles para todos los otros controladores de dominio del entorno. Los DCs que son incapaces de comunicarse con los controladores de dominio que aloja el FSMOs pueden experimentar errores.

Tarea 1: Ubicación del FSMO

En un bosque de dominio único, deje los cinco roles en un único servidor. No habría ningún beneficio en separarlos. Y seguramente se ganará en simplicidad e inversión en hardware.

En el dominio raíz de un bosque de múltiples dominios, deje todas las funciones de maestro de operaciones en el mismo controlador de dominio, siempre que todos los controladores de dominio del dominio raíz del bosque también sean servidores de catálogo global.

Si algunos de los controladores de dominio raíz del bosque no están configurados como servidores de catálogo global, es aconsejable mover la función de maestro de infraestructura a un controlador de dominio que no es un servidor de catálogo global y asegurarse de que el servidor no está configurado como tal. El papel de maestro de infraestructura no debe residir en un servidor de catálogo global a menos que todos los controladores de dominio en el dominio son servidores de catálogo global.

En todos los otros dominios, los tres roles de maestros de operaciones específicos de dominios pueden residir en el primer controlador de dominio de ese dominio. No es aconsejable colocar el papel de maestro de infraestructura en un controlador de dominio que es también un servidor de catálogo global.

Resumiendo, el FSMO debe ser colocado estratégicamente para garantizar el funcionamiento completo y adecuado de todos los servicios de directorio, tanto desde el punto de vista de la autenticación como también de la gestión. La ubicación del servidor FSMO debe ser decidida en base a cinco roles en el dominio raíz y en base a tres funciones para la totalidad de los restantes dominios en el bosque. Este proceso debe ser completado en forma detallada y a conciencia para cada bosque.

Tareas y consideraciones

Para cada función del maestro de operaciones, se debe elegir un controlador de dominio que puede albergar las funciones de maestro de operaciones. El maestro de operaciones que actúa como controlador de dominio de reserva debe ser un asociado de replicación directo del actual titular en esa función. Lo anterior se define con el fin de que el de reserva puede asumir el papel en caso de que el titular de un error. Este controlador que asume como titular de la función FSMO tendrá la información más actualizada del Servicio de Directorio.

Premisas de Diseño

Antes de comenzar con el paso C, es aconsejable leer detenidamente y entender profundamente las siguientes premisas de diseño:

Junto con la delegación administrativa, el arquitecto responsable del diseño del Servicio de Directorio debe entender los niveles de confianza entre los administradores que es inherente en diversos diseños del directorio.

- El propietario de un bosque controla los servicios y el acceso a los datos en todos los dominios en el bosque. Los propietarios del bosque de la empresa con derechos de acceso de administrador pueden recuperar siempre el control de los recursos a los cuales les han negado el acceso. Por esta razón, todas las organizaciones que participan en un bosque deben confiar implícitamente en el propietario del bosque.

- El propietario del dominio controla el acceso a los datos en el dominio y los que se encuentren almacenados en las computadoras que son parte del dominio. Por esta razón, las organizaciones que almacenan datos en OUs en el dominio o incorporan las computadoras a un dominio deben confiar en el propietario del dominio.

Puesto que el propietario del dominio también tiene acceso directo a los controladores del dominio que forman parte del dominio, hay una confianza implícita entre los propietarios del dominio que participan en el bosque junto con el propietario del bosque que confía en todos los propietarios del dominio. *Por ejemplo*, un propietario del dominio por error o quizás mal intencionadamente podría colocar un archivo binario modificado del sistema en el controlador del dominio que podría afectar la disponibilidad del servicio para todos los usuarios en el bosque.

Al quedar comprendidos los requisitos administrativos de la delegación, es posible comenzar a definir el número de bosques que la organización requiere. El arquitecto responsable de diseño del Servicio de Directorio debe identificar un bosque nuevo si existe cualquiera de los tres panoramas siguientes:

- **Aislamiento de servicio:** Un departamento o unidad de la organización requiere que ningún administrador fuera del departamento interfiera con la operación del Servicio de Directorio. El requisito para el aislamiento del servicio se basa generalmente en seguridad operacional o requisitos legales. Por ejemplo, considere una aplicación basada en directorio que apoye un proceso

de fabricación estrechamente controlado. Si la aplicación de directorio se despliega en un dominio dentro de un bosque, sería posible que el propietario del bosque, inadvertidamente o no, interrumpa la disponibilidad del Servicio de Directorio para el dominio de fabricación. Esto podía ocurrir por cancelación de sitios, quitando la información de configuración del dominio del contenedor de la configuración, o cambiando el esquema. Esta interrupción del servicio podía causar la falla de la aplicación de fabricación.

- **Autonomía de servicio a nivel de bosque:** Un requerimiento de conceder la habilidad a múltiples participantes de modificar los datos a nivel de bosque, tales como el esquema, independiente uno de otro. Este requisito se basa generalmente en la estructura de la organización o requisitos operacionales. Un ejemplo de esto serían dos aplicaciones que utilizan la misma clase y nombre de atributo pero lo definen de diferente manera. Debido a que hay solamente un esquema en un bosque, la única manera de aislar los esquemas uno de otro es ubicándolos en diferentes bosques. Este panorama es algo inusual, pero es bueno contemplarlo a modo de ejemplo de interpretación del diseño.

- **Aislamiento de datos del propietario del servicio:** Una organización requiere que el propietario del dominio prevenga el acceso a los datos almacenados en el dominio por los propietarios del servicio del bosque. Este requisito se basa generalmente en requisitos legales. Por ejemplo, considere un requisito legal que solamente la gente perteneciente a un departamento específico dentro de la organización puede tener acceso a los datos almacenados en un dominio. Si el dominio fuera desplegado como dominio separado dentro de un bosque, no habría manera de hacer cumplir este requisito ya que un administrador de la empresa puede eliminar cualesquiera ajustes de la seguridad puestos por un administrador del dominio.

Crear bosques adicionales puede ser costoso para una corporación y debe ser emprendido solamente cuando es necesario. Incluso si los costos de hardware y software que resultan se consideraran insignificantes o manejables, los costos administrativos asociados serán altos. Si un bosque adicional es agregado debido a los requerimientos de la organización, debe analizarse el balance de los costos implicados con las ventajas ganadas. Mientras que un departamento pude preferir operaciones autónomas del servicio, puede ser que sea más rentable poner en

ejecución políticas apropiadas de seguridad y/o centralizar la responsabilidad de la disponibilidad del servicio centralizando en un grupo confiable de TI.

El propietario del bosque debe delegar dominios si hay una necesidad de autonomía a nivel del servicio de dominio. Disponibilidad del servicio (para el dominio), relaciones de confianza externas, y políticas de cuenta de usuario del dominio son los elementos del servicio del directorio que son controlados a nivel de dominio. El propietario del bosque puede delegar la administración de un dominio que requiera la autonomía del servicio para estos aspectos de disponibilidad del servicio.

Si se requiere la autonomía o el aislamiento de los datos, un propietario del dominio puede delegar la administración de una OU al propietario de dichos datos. Los requisitos organizacionales u operacionales crean típicamente necesidad de este tipo de aislamiento de los datos. Por ejemplo, considere un departamento pequeño que posea un servidor local y desee controlar que los usuarios tengan acceso a sus recursos. Además, el departamento puede desear publicar las partes en el directorio de modo que los clientes puedan localizarlas a través de Active Directory. Si no hay requisito para negar el acceso administrativo a los propietarios del bosque o del dominio, delegar la administración de OU es suficiente para apoyar los requisitos administrativos de los departamentos o unidades dentro de las organizaciones.

Paso C1: Crear el Diseño del Sitio

El diseño del sitio consiste en el mapeo de la red física en la construcción del sitio lógico 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 activo 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 relacionados con el directorio, y por lo tanto pueden ser ubicados lógicamente más cercanos de estos recursos.

Las siguientes decisiones son necesarias realizar:

- ¿Se correlaciona una localización física con un sitio?
- ¿Puede una ubicación física agruparse con otras ubicaciones en un sitio?

Una vez que los sitios han sido identificados, las tarea final será mapear las subredes TCP/IP representadas en una ubicación específica en el sitio correspondiente. De ser necesario el diseño del sitio se puede cambiar posteriormente.

Tarea 1: Crear un sitio para la localización

Un sitio debe definirse para cualquier ubicación física en la que los controladores de dominio están localizados, así como cualquier lugar físico que contiene recursos o servicios que dependen de la topología de la información del sitio para dirigir el cliente al recurso solicitado más cercano.

Por ejemplo, si varias ubicaciones físicas necesitan acceder a recursos de archivo, estos recursos pueden ser configurados en un entorno de sistema de archivos distribuido (DFS, en inglés *Distributed File System*) de medio ambiente. Después de colocar los servidores DFS que contienen los recursos en los lugares físicos, un sitio puede ser configurado para cada ubicación. Cuando un cliente accede a los recursos basados en DFS, accederá al recurso DFS local. De esta forma reducirá el tráfico sobre los vínculos WAN/MAN, mejorando el rendimiento del acceso a los recursos.

Por último, los sitios pueden ser creados para administrar que controladores de dominio atienden el tráfico de validación de aplicaciones que poseen requerimientos de autentificación muy elevados.

Es importante documentar también en esta etapa para cada sitio identificado, el nombre del sitio y las subredes IP que se asignan al mismo.

Tarea 2: Asociar la ubicación más cercana al Sitio definido

Para cualquier localidad física restante que no ha sido asociada a un sitio en Active Directory, asociar las subredes de esa ubicación a un sitio existente. El sitio seleccionado debe incluir un lugar que posea la mayor velocidad de WAN/MAN y ancho de banda disponible para la ubicación que se está configurando. Este enfoque permitirá direccionar el tráfico de clientes generado dentro de la ubicación hacia el sitio que posee la mayor capacidad para manejar el tráfico adicional.

Documente la información de asignación de subredes adicionales al sitio seleccionado.

En resumen, se debe examinar cada ubicación física y decidir respecto a si debe ser un sitio nuevo en el directorio o se debe asociar a uno ya existente. Las subredes dentro de cada lugar deben ser asignadas al sitio al que pertenecen. Cada controlador de dominio también debe ser asignado al sitio adecuado.

El diseño de sitios debe ser completado para cada uno de los bosques

.

Paso C2: Crear el Diseño de Vínculos a Sitios

Los vínculos de sitios se utilizan para conectar los sitios definidos en Active Directory. Los vínculos del sitio reflejan la conectividad entre los sitios y el método utilizado para transferir el tráfico de replicación. Todos los sitios deben estar conectados con vínculos de sitios si los controladores de dominio en cada sitio se replican. Por defecto, todos los sitios pertenecen al vínculo del primer sitio determinado, con la replicación programada cada 180 minutos, cada día de la semana.

Se pueden crear vínculos de sitios en cualquier momento y los sitios se pueden, fácilmente, añadir o quitar. Sin embargo, podría haber un impacto en la replicación, debido a problemas de latencia cuando se reconfiguran los sitios, vínculos de sitios, y la planificación asociada con los vínculos del sitio.

Tarea 1: determinar el Diseño de los Vínculos de Sitio

Active Directory crea automáticamente el primer vínculo de sitio predeterminado. Cuando todos los sitios en el diseño están conectados y tienen la misma conectividad y disponibilidad unos a otros, un vínculo de sitio simple puede ser usado para representar los vínculos entre los sitios. Este diseño de malla completa supone que todos los sitios están bien conectados y que no es necesario el diseño de vínculos específicos entre sitios. Este enfoque simplifica el diseño, eliminando la necesidad de diseñar vínculos de sitios, así como la configuración automática de la estructura de vínculos de sitios.

Dado que la conectividad y la disponibilidad de los vínculos son idénticos, la programación de replicación, intervalo, y el costo será configurado de forma idéntica. Esta opción sólo es útil cuando todos los sitios están conectados por conexiones WAN con idéntico ancho de banda disponible y latencia.

Si los sitios están conectados con vínculos de red física que tienen distintos costos de uso, disponibilidad, velocidad, o ancho de banda disponible, puede existir la necesidad de una programación de replicación diferente. Un vínculo de sitio nuevo tendría que ser creado para reflejar estas diferencias.

Los vínculos de sitios utilizan un algoritmo de costos para influir en los que el tráfico de replicación de ruta a utilizar para el flujo entre los sitios. Una conexión más óptima sería configurada con un costo menor que una conexión de menos óptima. El sistema de replicación utiliza el vínculo con el menor costo. Si hay un costo en dólares

a la utilización de un vínculo, el vínculo podría ser asignado un valor de costo más alto también.

El tráfico de replicación a través del vínculo está controlado por la planificación de disponibilidad y la frecuencia con que el vínculo se establece para replicar. Por ejemplo, un vínculo se puede configurar para replicar cada 30 minutos desde las 2:00 a las 4:00, de lunes a viernes.

La programación del sitio puede especificar intervalos tan breves como pueden ser cada 15 minutos. Estos rangos se pueden definir en cualquiera de las 24 h horas, y cualquier combinación de días de la semana.

Al asignar los horarios y los intervalos de replicación, se debe tener cuidado para garantizar que se cumplen todos los objetivos de la replicación requerida por la organización. Los objetivos de réplica se pueden definir de tal manera que todos los cambios que se registran en un período determinado de tiempo para lo siguiente:

- **Convergencia de configuración y esquema.** Cualquier cambio de configuración o en el esquema se replican en todos los controladores de dominio en el bosque.
- **Convergencia de dominio.** Todos los cambios de dominio se replican en todos los controladores de dominio en el dominio.
- **Convergencia de catálogo global.** Todos los cambios de catálogo global se replican en todos los catálogos globales en el bosque.
- **Convergencia de partición de la aplicación.** Todos los cambios en la partición de la aplicación se replican en todos los controladores de dominio que alberga la partición de la aplicación afectada.

Al definir la planificación e intervalos de replicación, asegúrese de que todos los objetivos de la replicación se cumplen en los peores escenarios posibles. Es decir, ¿Un cambio originado en un sitio réplica en el plazo de tiempo con el sitio que está al mayor número de saltos del sitio de origen? Si no es posible alcanzar el objetivo, el intervalo y el calendario necesitan ser revisados o el objetivo debe ser redefinido.

Considere la posibilidad de una topología que consta de cinco sitios (A-F), que consiste en un único bosque, con cuatro dominios. Los sitios están conectados entre sí a través de vínculos de sitios directos con la programación de replicación configurado

por 24 horas y el conjunto de intervalo en el valor predeterminado de 3 horas. A los efectos de este ejemplo, hay dos objetivos de la replicación: una para el esquema y la convergencia de configuración para ser completado en 6 horas y otro para la convergencia de catálogo global en 4 horas.

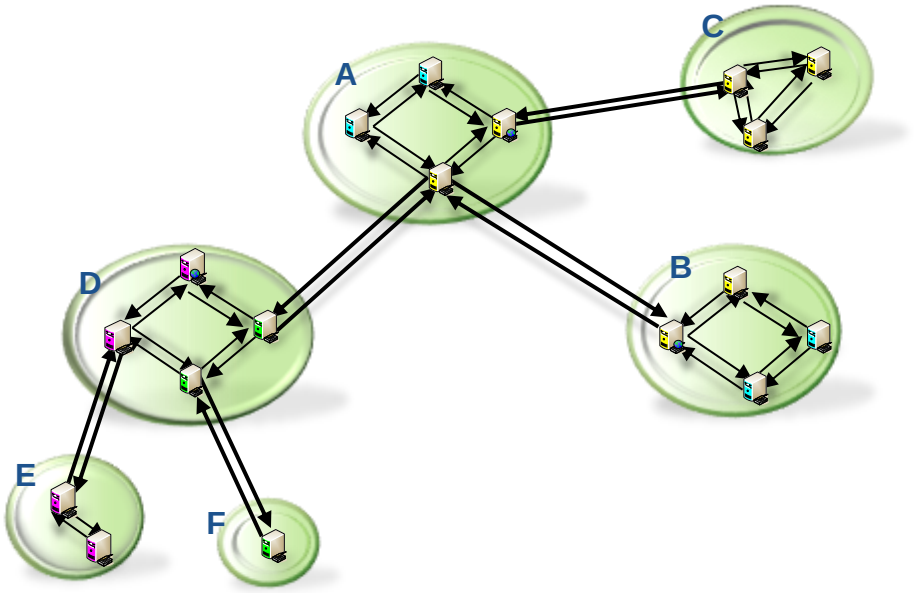

Ilustración 11. Configuración del esquema de convergencia.

Debido a la cantidad de saltos que intervienen, no es posible que un cambio introducido en el sitio E o F pueda converger hacia el sitio C en 6 horas; se necesitaría un mínimo de 9 horas (3 saltos). O bien el objetivo de replicación tendría que ser actualizado o sería necesario establecer otro valor para el intervalo.

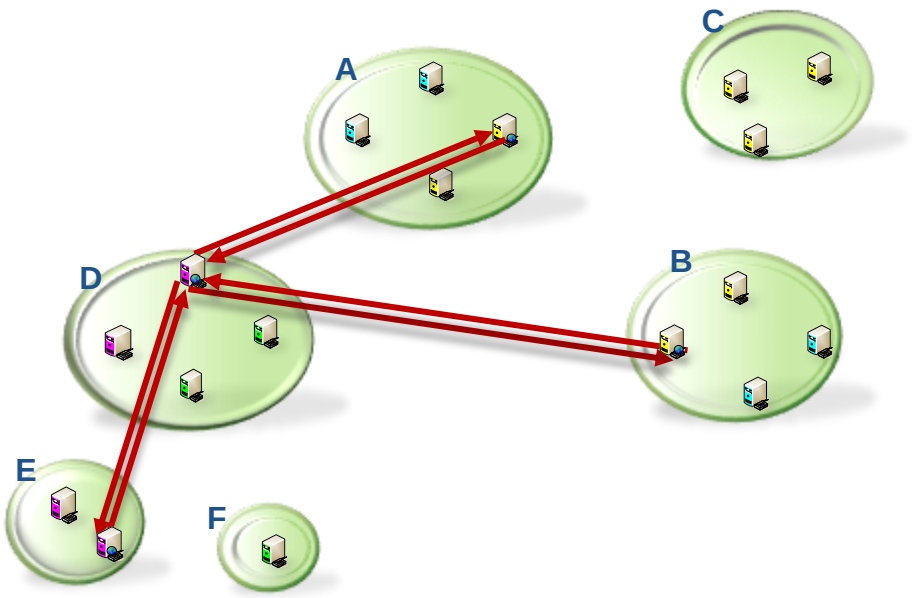

Ilustración 12. Convergencia de Catálogo Global.

En el ejemplo de la convergencia de catálogo global, hay cuatro servidores de catálogo global en los sitios A, B, D y E. Si un cambio es introducido en el sitio D, entonces todos los sitios se actualizarán dentro del objetivo de 4 horas. Sin embargo, si el cambio se realice en los sitios A, B o E, entonces no será posible alcanzar el objetivo de 4 horas ya que tendrá un mínimo necesario de 6 horas (2 saltos) para llegar a todos los sitios. Una vez más, los objetivos de la replicación tendrían que ser actualizados o el intervalo de tiempo debería ser modificado en los vínculos de sitio.

Asociando todos los sitios con vínculos similares con el nuevo vínculo y eliminar los sitios del vínculo de sitio predeterminado.

Para cada vínculo de sitio identificado, documentar el nombre, el costo asociado con el uso del vínculo, y el intervalo y programación de la replicación del mismo. Por cada sitio documentar también, el vínculo registro que se utiliza para conectar a otros sitios. Un sitio puede disponer múltiples vínculos a sitios asociados a él.

En resumen, los vínculos entre todos los sitios se deben definir mediante el uso de uno o más vínculos de sitios. Si algunos sitios están desconectados de los demás, el Comprobador de Coherencia de Réplica (KCC, en inglés *Knowledge Consistency Checker*) generará un mensaje de error. Los vínculos de sitios controlan la replicación de la base de datos del directorio entre los controladores de dominio en sitios diferentes. Y, si se dispone de varias rutas de acceso, el controlan que camino es el preferido.

El diseño de los vínculos de sitios se puede cambiar. Sin embargo, cambiarlos puede tener impacto en la propagación de los cambios del directorio hasta que converjan todas las actualizaciones.

Paso C3: Crear el Diseño de Puentes de Vínculos a Sitios

Un puente de vínculo a sitio permite transitividad entre vínculos a sitios. Cada vínculo a sitio en un puente tiene que tener un sitio en común en lo referido a la replicación, para que fluya correctamente a través del puente. El diseño de un puente de vínculo a sitio se puede cambiar, pero debe hacerse cuidadosamente para evitar que la replicación de Active Directory no se vea comprometida o no pueda efectuarse.

Opción 1: Comportamiento predeterminado

Si la red está completamente ruteada y no hay necesidad de controlar el flujo de replicación de Active Directory, entonces deje la transitividad habilitada para todos los vínculos de sitio dejando la opción de puente a todos los vínculos a sitios habilitada. Este es el estado por defecto.

Al permitir la transitividad a través de todos los sitios, cualquier controlador de dominio en un sitio puede crear un asociado de replicación directo con otro controlador de dominio en otro sitio. Esto simplifica la replicación ya que no hay necesidad de limitar o definir los sitios que un controlador de dominio puede utilizar para la búsqueda de asociados de replicación.

Esto puede convertirse en un problema con las implementaciones más grandes que se basan en una topología tipo estrella. Al construir puentes entre todos los vínculos de sitio, no hay control en cuál controlador de dominio se considera parte del sitio central cuando se trata de una réplica.

Opción 2: Personalizar un puente de vínculo de Sitio

Si la red no es completamente ruteada, es aconsejable deshabilitar la opción “Puente entre todos los vínculos de sitio” (en inglés *Bridge All Site Links*) para el transporte IP y configure puentes de vínculos de sitios para mapear las conexiones físicas de redes. Adicionalmente, si la red IP es totalmente ruteada, pero hay muchas rutas que el KCC no debe considerar, creando una topología de puentes de vínculos de sitios personalizada y desactivando la transitividad automática de vínculos de sitios puede ayudar a eliminar la confusión. El KCC, por defecto, tendrá en cuenta todas las conexiones posibles y los puentes para la replicación.

Puentes de vínculos de sitios también se puede utilizar para controlar el flujo de replicación de Active Directory. Las dos razones más comunes para la creación de puentes de vínculos de sitios son para controlar a replicación ante la conmutación por error en el diseño de red con topología estrella y el control de la replicación a través de

un firewall. Si el flujo de replicación de Active Directory se controla a través del diseño de puentes de vínculo de sitio, desactive la opción “Puente entre todos los vínculos de sitio” para el transporte IP.

Mediante la configuración de dos puentes de vínculo de sitio para la replicación de Active Directory entre los dos sitios, la réplica tendrá éxito incluso si un vínculo falla. Esto es necesario porque la desactivación de la opción “Puente entre todos los vínculos de sitio” negará al KCC y al generador de topología entre sitios (ISTG) de ayudar con el puente de vínculos a sitios en el caso de un fallo en cualquier aspecto de la topología.

Si el tráfico de replicación pasa a través de un firewall y el firewall está configurado para permitir conexiones desde los controladores de dominio específico, entonces los puentes que unen los sitios deben ser configurados para que coincidan con este entorno. Un puente de vínculo de sitio se debe crear a cada lado del servidor de seguridad. El vínculo de sitio que conecta los dos sitios a través del firewall no debe ser colocado en el puente. Si un controlador de dominio que se le permite comunicarse a través del servidor de seguridad falla, sus asociados de replicación intentarán establecer nuevos asociados de replicación sólo con los controladores de dominio en los sitios que forman parte del puente.

Cabe señalar que la solidez de la replicación de Active Directory puede ser reducida por las opciones que se adopten. Por ejemplo, si todos los controladores de dominio ubicados en el centro de una topología tipo estrella fallan, los sitios satélites será desconectado de la topología de replicación, ya que todos sus socios potenciales han sido eliminados de la red.

Del mismo modo, si los controladores de dominio que se comunican a través del servidor de seguridad fallan, entonces la replicación actualizará únicamente los cambios que se realizan en ambos lados del firewall. Las modificaciones no cruzarán el servidor de seguridad hasta que los controladores de dominio sean puestos nuevamente en línea.

Evaluación de las características

Complejidad		
Configuración de Puente de Vínculos de Sitios por defecto	Usando la configuración por defecto se alcanza una implementación menos compleja.	Bajo
Configuración de Puente de Vínculos de Sitios personalizada	Personalizando la configuración aumenta la complejidad del entorno.	Alto

Tabla 13. Análisis de complejidad en diseño de puentes de vínculos de sitios.

En resumen, los puentes de vínculos de sitios pueden ser configurados y la configuración por defecto cambia sólo cuando la red requiere modificaciones. Todos los sitios deben estar interconectados entre sí, ya sea directamente o a través del puente.

La decisión de establecer o cambiar los puentes vínculo de sitio puede ser revisada permanentemente.

Es importante documentar cualquier de puente de vínculo de sitio que se crean y los vínculos de sitios asociados a ese puente.

Paso D1: Determinar la Configuración del Controlador de Dominio.

Una vez que el número de controladores de dominio ha sido identificado, el paso final es determinar el espacio en disco, memoria, CPU, y requisitos de red para cada controlador de dominio.

Tarea 1: Identificar los requisitos mínimos de espacio en disco para cada controlador de dominio:

Para cada controlador de dominio va a destinar, como mínimo, la siguiente cantidad de espacio:

- 500 MB para los registros de transacciones de Active Directory (*transaction Log*).
- 500 MB para la unidad que contiene el recurso compartido “SYSVOL”.
- 1,5 GB a 2 GB para los archivos del sistema operativo Windows Server 2008.
- 0,4 GB de almacenamiento por cada 1.000 usuarios en el directorio de la unidad de Ntds.dit.

Por ejemplo, en un bosque con dos dominios (el dominio A, y el dominio B), con 10.000 y 5.000 usuarios, respectivamente, prever un mínimo de 4 GB de espacio en disco para cada controlador de dominio que aloja el dominio A y un mínimo de 2 GB de espacio en disco para cada controlador de dominio que aloja dominio B.

Los controladores de dominio que se ejecutan como servidores de catálogo global necesitan asignar espacio adicional en disco si el bosque contiene más de un dominio. Para un determinado servidor de catálogo global, la necesidad de espacio adicional es de 50% del espacio de disco recomendado para cada dominio adicional fuera del dominio del propio servidor de catálogo global. En el ejemplo anterior, el dominio A requiere 4 GB de espacio en disco y el dominio B requiere 2 GB de espacio en disco. Para un servidor designado como catálogo global en el dominio A, se necesitará un adicional de 1 GB (Dominio B´s 2 GB / 2), para un total de 5 GB de almacenamiento. Para un servidor de catálogo global en el dominio B, se necesitarán un adicional 2 GB (Dominio A´s 4 GB / 2), para un total de 4 GB de espacio en disco.

Por último, si las aplicaciones están utilizando el directorio para almacenar datos en una partición de aplicación, los requisitos de almacenamiento para cada partición

de aplicación tendrán que ser añadido a los requisitos de disco del controlador de dominio.

La Identificación de requerimientos de capacidad es un elemento en la planificación de la configuración de espacio de disco. El segundo elemento es la planificación del rendimiento. El subsistema de disco necesita ser configurado para leer y escribir datos a una velocidad que responda a las expectativas de rendimiento de los objetivos organizacionales. Algunos de los tipos de RAID se pueden utilizar para ofrecer tolerancia a fallos y disponibilidad.

Para los sitios más pequeños, un solo disco puede satisfacer tanto las necesidades de capacidad y como las de rendimiento. Para los grandes sitios, los registros (*logs*), el sistema operativo y los archivos de base de datos puede ser necesario colocar en los volúmenes por separado a fin de cumplir los requisitos de rendimiento. Es necesario probar la configuración para asegurarse que el subsistema de disco no es un cuello de botella con la carga esperada.

Es aconsejable documentar las configuraciones de las unidades determinadas para cada servidor.

Tarea 2: Identificar los requisitos de memoria para cada controlador de dominio:

La siguiente tabla da una estimación conservadora de la dotación mínima de memoria requerida para un controlador de dominio. El cuadro supone que los controladores de dominio sólo albergan Directorio Activo y DNS.

Usuarios por Dominio en un Sitio	Requisitos mínimos de memoria por controlador de dominio
001 – 499	512 MB
500 – 999	1 GB
> 1.000	2 GB

Tabla 14. Asignación de memoria mínima requerida.

En este cuadro se expresan mínimos, memoria adicional puede mejorar el rendimiento del Servicio de Directorio. Active Directory intenta generar un caché de la

base de datos en memoria. Esto reduce el acceso a disco y mejora el rendimiento. Esta caché está limitado por el espacio de direcciones virtuales y la cantidad de RAM física en el servidor.

Si no hay una infraestructura ya existente, medir el rendimiento de los controladores de dominio para determinar la memoria existente es suficiente para el medio ambiente. Si se trata de un despliegue nuevo, es aconsejable comenzar con 2 GB de RAM. Probar la configuración con las cargas de procesamiento esperadas y agregar memoria según sea necesario.

Una de las formas para determinar si es necesario colocar más memoria RAM en el servidor definido como DC es controlar el porcentaje de operaciones de Active Directory que se han cumplido desde la memoria caché mediante el Monitor de confiabilidad y rendimiento. Examine la instancia del lsass.exe (del servicio de dominio de Active Directory) o la instancia de Directorio (del servicio de Active Directory *Lightweight Directory*) del contador de rendimiento de la base de datos de aciertos de caché de base de datos. Un valor bajo indica que muchas operaciones no han sido satisfechas desde el caché; añadir más memoria RAM puede mejorar la tasa de aciertos de caché y el rendimiento de Active Directory. Se debe examinar este contador después de que Active Directory ha estado funcionando por algún tiempo bajo una carga de trabajo normal. El caché empieza vacía cuando el servicio Active Directory se reinicia o se reinicia el servidor, por lo que la tasa de éxito inicial es naturalmente bajo.

El uso de caché de la base de datos es la mejor forma de evaluar las necesidades de memoria RAM de un servidor. Alternativamente, una guía es que cuando la memoria RAM en un servidor es el doble del tamaño físico de la base de datos de Active Directory en el disco, es probable que le dé suficiente espacio para almacenamiento del caché de la base de datos en la memoria. Sin embargo, en muchos escenarios se trata de una sobreestimación, porque la parte real de la BD más utilizada es sólo una fracción de la misma.

Tarea 3: Determinar los requisitos de la CPU

Un servidor de 32 bits que se ejecutan la versión estándar de Windows Server 2008 sólo puede direccionar 4 GB de RAM. Si existiese la necesidad de crecimiento de la RAM en un servidor en más de 4 GB, se debería pensar en una arquitectura de 64-bits. Al cambiar hacia una versión de 64 bits de Windows Server 2008 o 2008 R2, la capacidad de expansión futura del sistema está protegida.

En esta guía se supone que la carga primaria de los controladores es la autenticación de usuarios. En el caso de que se levantaran otros roles o si los servidores procesan solicitudes adicionales, es sano supervisar el rendimiento del sistema y ajustar el número de CPU según sea necesario. Si ya existen controladores de dominio en el medio ambiente, la información de control de estos puede ser útil para obtener una línea de base inicial sobre el hardware necesario a futuro.

Es importante documentar el número de CPUs y la arquitectura elegida para cada controlador de dominio.

Tarea 4: Identificar los requisitos de la red para cada controlador de dominio:

Muchas redes corporativas funcionar a 100 megabit o gigabit hacia los servidores. Normalmente, un único adaptador de red es suficiente para manejar todo el tráfico de red desde y hacia el servidor.

La instalación de varios adaptadores de red (NIC) en un controlador de dominio puede causar ciertos inconvenientes, que pueden ser errores de replicación o de autenticación. Por lo anterior no se recomienda esta práctica para entornos de PyMO.

Tareas y consideraciones

Active Directory está optimizado para escenarios pesados en lectura, es decir, cuando la carga de trabajo se compone mayoritariamente de operaciones de consultas que de operaciones de actualización. La consideración más importante en cuanto a sintonía fina es garantizar que el servidor tiene suficiente RAM para poder almacenar en caché (memoria) la porción de la base de datos usada frecuentemente. Mediante el control de la base de datos de aciertos de caché en el servidor, se puede determinar si la memoria adicional es necesaria. Tener en cuenta lo ya expuesto. El porcentaje de muestras será bajo si el Servicio de Directorio fue inicializado recientemente.

En escenarios opuestos, pesados en escritura, es importante optimizar el subsistema de almacenamiento para mejorar el rendimiento. Uso de los controladores RAID por hardware de baja latencia, los discos de altas RPM, y de escritura respaldada por caché en el controlador puede ayudar a mejorar el rendimiento. Debido a que mayoritariamente la carga de trabajo consta de escrituras, el caché no proporciona tantos beneficios como en los escenarios pesados en lectura.

En resumen, la configuración física adecuada de los controladores de dominio es esencial para el buen funcionamiento de Active Directory. Elementos críticos incluyen

el subsistema de disco, memoria, CPU, y adaptadores de red. El hardware puede ser reconfigurado como sea necesario, pero hacerlo puede requerir cierta planificación y cortes en el servicio.

CAPÍTULO IV: CONCLUSIONES Y POSIBLES AMPLIACIONES

CONCLUSIONES

A lo largo del desarrollo de la propuesta de este trabajo, se le ha dado especial énfasis al desarrollo de un flujo de trabajo guiado, debidamente documentado y adecuadamente contextualizado en el ámbito de una Organización Mediana. Si bien, la base sobre la cual se ha trabajado es una de las guías de la arquitectura de referencia IPD del fabricante del Servicio de Directorio Active Directory, se ha complementado con abundante información adicional relacionada con el contexto de este tipo de organizaciones, y con la experiencia del autor en lo referente al diseño de este tipo de servicios.

El hecho de que las OMs, poseen como característica distintiva un staff de TI muy particular (los “Informáticos Generalistas”), su presupuesto limitado y la complejidad creciente de la tecnología enfocada bajo los objetivos organizacionales presentan una realidad bastante particular y exigente.

Es crucial entender y reconocer el problema o la familia de problemas relacionados producto de la evolución y desarrollo de los objetivos organizacionales. Contar con ciertas guías, la cuales han sido desarrolladas en base a experiencia y con un conocimiento concreto de la tecnología a emplear, es algo fundamental en los entornos empresariales modernos. En este momento es bueno entender el alcance de la máxima “no re inventar la rueda”, al momento de gestionar un ambiente en permanente cambio y evolución.

El Servicio de Directorio es uno de los servicios fundamentales y extremadamente sensibles dentro de la infraestructura TI en las organizaciones modernas. El poder cubrir el ciclo de vida completo de este servicio, de una forma ordenada y controlada sin dudas es un objetivo altamente deseable de alcanzar por cualquier organización.

Este trabajo, pretende humildemente aportar ciertas bases a la hora de definir una metodología de despliegue de servicios de TI y comenzar a construir parte de la cultura organizacional en lo referido a la gestión de Tecnologías de la Información en las organizaciones medianas modernas.

POSIBLES AMPLIACIONES

A continuación se presentan un conjunto de posibles futuros trabajos, en el área de la Gestión de la Tecnología de la Información.

- Completar el ciclo de vida del Servicio de Directorio de Microsoft (Active Directory), o algunas de sus etapas, mediante el empleo de Arquitecturas de Referencia.
- Diseño de otros Servicios de Directorios, basados en Arquitecturas de Referencia de otros proveedores.
    - Se propone adoptar la AR propuesta por Novell para su Servicio de Directorio eDirectory.
    - Alternativa de RedHat, basada en LDAP para su ecosistema.
- Desarrollo de un servicio de MetaDirectorio. Este trabajo es bastante específico, pero permite resolver la integración de ecosistemas tecnológicos mediante un “puente”, como puede ser un servicio de MetaDirectorio.

Bibliografía

HOWES, T., GOOD, G. S., & SMITH, M. (2003). *Understanding and deploying LDAP directory services.* Pearson Addison Wesley.

Microsoft. (2003). *Windows Server System Reference Architecture.* Recuperado el 01 de Julio de 2010, de Architecture Blueprints: http://www.microsoft.com/en-us/download/details.aspx?id=15777

Microsoft. (2007). *El viaje de Optimización de Infraestructura de Micrtosoft.* Recuperado el 15 de Diciembre de 2012, de http://www.microsoft.com/latam/technet/infraestructura/optimizacion.mspx

Microsoft. (2008). *Windows Server 2008 Deployment Kit.* Recuperado el 13 de Julio de 2012, de Designing and Deploying Directory and Security Services: http://www.microsoft.com/en-us/download/details.aspx?id=32299

Microsoft. (2009). *Active Directory Domain Services.* Recuperado el 01 de Mayo de 2012, de http://technet.microsoft.com/en-us/library/cc268216.aspx

Microsoft. (2010). *Serie de Soluciones de informática para empresas medianas.* Recuperado el 21 de Diciembre de 2011, de http://www.microsoft.com/latam/technet/mediana/51-250/intro/mit_intro_1.mspx

Ministerio de Industria. (Febrero de 2013). *Ministerio de Industria de la Nacion*. Recuperado el 23 de Febrero de 2013, de Secretaría de la Pequeña y Mediana Empresa y Desarrollo Regional: http://www.sepyme.gob.ar/sepyme/clasificacion-pyme

Solutions Accelerators. (Octubre de 2009). *Infraestructure Planning and Design.* Recuperado el 03 de Diciembre de 2012, de Series Introductions: http://www.microsoft.com/IPD

x500 Standard. (2001). *The website of the X.500 Directory standard*. Recuperado el 07 de Enero de 2012, de http://www.x500standard.com/index.php?n=Ig.History

Nota: Para las citas y referencias se empleó el estilo de la “AMERICAN PSYCHOLOGICAL ASSOCIATION” (A.P.A.)

Listado de Tablas

N° Descripción Pag.

Listado de Ilustraciones

N° Descripción Pag.

Glosario

Aclaración importante: en el presente trabajo, se ha intentado mantener las siglas en inglés. Lo anterior es debido a que por ser este el lenguaje nativo empleado en la documentación técnica asociada a la informática, se facilita la búsqueda y asociación de información a partir de siglas en este idioma. El trabajar con traducciones de las mismas, suele producir ambigüedades y confusiones.

[A]

Active Directory - AD: Ver Directorio Activo.

[B]

Bosque de AD: Es la agrupación de varios árboles de dominio en una estructura jerárquica. También se lo puede entender como una colección de árboles esencialmente iguales, sin una única raíz en el espacio de nombres.

[C]

Catálogo Global – GC (en inglés *Global Catalog*): Es un componente que permite a usuarios o aplicaciones poder encontrar objetos en un árbol de dominio de AD. Contiene una copia de cada objeto de AD pero con solo un pequeño número de atributos. Los atributos en GC son utilizados para las operaciones de búsqueda y/o para encontrar una copia completa de un objeto. El catálogo global está integrado en el sistema de réplicas de AD.

Conjunto Redundante de Discos Independientes - RAID (en inglés *Redundant Array of Independent Disks*): Originalmente *Redundant Array Inexpensive Disks*, traducido como “Conjunto Redundante de Discos Independientes”, hace referencia a un sistema de almacenamiento de datos que usa múltiples unidades de almacenamiento de datos (discos duros o SSD) entre los que se distribuyen o replican los datos. Dependiendo de su configuración (a la que suele llamarse “nivel”), los beneficios de un RAID respecto a un único disco son uno o varios de los siguientes: mayor integridad, mayor tolerancia a fallos, mayor rendimiento (en inglés *throughput*) y mayor capacidad. En sus implementaciones originales, su ventaja clave era la

habilidad de combinar varios dispositivos de bajo coste y tecnología más antigua en un conjunto que ofrecía mayor capacidad, fiabilidad, velocidad o una combinación de éstas que un solo dispositivo de última generación y coste más alto.

En el nivel más simple, un RAID combina varios discos duros en una sola unidad lógica. Así, en lugar de ver varios discos duros diferentes, el sistema operativo ve uno solo. Los RAIDs suelen usarse en servidores y normalmente (aunque no es necesario) se implementan con unidades de disco de la misma capacidad. Debido al descenso en el precio de los discos duros y la mayor disponibilidad de las opciones RAID incluidas en los chipsets de las placas base, los RAIDs se encuentran también como opción en las computadoras personales más avanzadas.

Niveles RAID estándar:

• RAID 0 (Data Striping): También llamado conjunto dividido, volumen dividido o volumen seccionado. Distribuye los datos equitativamente entre dos o más discos sin información de paridad que proporcione redundancia.

• RAID 1 (Mirroring): Crea una copia exacta (o espejo) de un conjunto de datos en dos o más discos. Esto resulta útil cuando el rendimiento en lectura es más importante que la capacidad.

• RAID 5: Conjunto dividido con paridad distribuida, también llamado distribuido con paridad. Es una división de datos a nivel de bloques distribuyendo la información de paridad entre todos los discos miembros del conjunto. Este nivel de RAID ha logrado popularidad gracias a su bajo coste de redundancia.

Contenedor de AD: Es similar a un objeto de AD, puesto que posee atributos. Pero a diferencia de este no representa algo concreto. Es decir, puede ser un almacén de objetos y de otros contenedores de AD.

[D]

Directorio Activo – AD (en inglés *Active Directory*)**:** Es el término que emplea Microsoft para referirse a su producto de Servicio de Directorio para una red distribuida de dispositivos computacionales. Emplea numerosos protocolos, entre los más destacados se encuentran: LDAP, DNS, DHCP y Kerberos. En forma simple, se puede definir como un servicio establecido en uno o varios componentes servidores donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los

inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en el resto de la red. Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso. También permite a los administradores establecer políticas a nivel de organización, desplegar programas en muchos ordenadores y distribuir actualizaciones críticas a una organización entera. AD almacena información de una organización en una base de datos central, organizada y accesible. Pueden encontrarse desde directorios con cientos de objetos para una red pequeña hasta directorios con millones de objetos.

DN - Distinguished Name: Ver Nombre Distinguido.

DNS - Domain Name System: Ver Sistema de Nombres de Dominio.

[E]

Esquema de AD: En AD, el esquema son todos los fragmentos que lo componen, como pueden ser: objetos, atributos, contenedores, entre otros. AD posee un esquema predeterminado que define la mayoría de las clases de objetos habituales tales como: usuarios, grupos, computadoras, departamentos, políticas de seguridad y dominios. El esquema puede ser actualizado dinámicamente, ya sea mediante la creación o modificación de algún objeto.

Exchange Server (Exchange): Es un sistema de mensajería propietario de Microsoft que incluye un servidor de correo, un programa de correo electrónico (cliente de correo electrónico) y aplicaciones de trabajo en grupo. Exchange fue diseñado para uso en un entorno comercial corporativo. El servidor de Exchange se utiliza a menudo en conjunto con Microsoft Outlook para aprovechar las características de colaboración de este, tales como la capacidad para compartir calendarios, tareas, listas de contactos. Microsoft Exchange Server tiene dos propósitos principales:

- Soporte a mensajería: SMTP, POP, IMAP, web mail, así como su propio cliente de correo Microsoft Outlook.
- Soporte a trabajo colaborativo: mediante Outlook en sus escritorios o Outlook Web Access a través de un navegador web.

[F]

Firewall: Suele traducirse en español como “cortafuego”. Es un sistema computacional que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Puede tratarse de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos (subredes) sobre la base de un conjunto de normas y otros criterios. Los cortafuegos pueden ser implementados en hardware o software, o mediante una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuego, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar el cortafuego a una tercera red, llamada “zona desmilitarizada” o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

FSMO - Felxible Single Master Operation: Ver Maestro de Operaciones.

[G]

GC - Global Catalog: Ver Catálogo Global.

GPO - Group Policy Objects: Ver Objetos de Política de Grupo.

[I]

IMS - IP Multimedia Subsystem: Ver Subsistema Multimedia IP.

Instrumentación para la Administración de Windows – WMI (en inglés *Windows Management Instrumentation*): Es la fuente principal para administrar los datos y la funcionalidad en equipos locales y remotos que ejecutan los sistemas operativos Microsoft Windows. Puede obtener los datos de administración de WMI directamente a través de scripts y aplicaciones o a través de herramientas de administración corporativas como Microsoft Systems Management Server (SMS) y Microsoft Operations Manager (MOM). Puede utilizar scripts escritos en cualquier lenguaje de scripting que pueda funcionar con Windows Script Host. WMI es la implementación de Microsoft de WBEM (en inglés Web-Based Enterprise Management), una iniciativa del sector para establecer estándares que sirvan para obtener acceso y compartir información de administración a través de una red corporativa. WMI es compatible con WBEM y ofrece compatibilidad integrada con CIM (en inglés Common Information

Model), el modelo de datos que describe objetos que existen en un entorno de administración corporativo. Ejemplos de otros enfoques de gestión de sistemas serían los *shell* remotos, soluciones propietarias y arquitecturas de gestión de red como SNMP.

ITU-T: (en inglés *International Telecomunication Union - Telecomunication*) El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es el órgano permanente de la Unión Internacional de Telecomunicaciones (UIT) que estudia los aspectos técnicos, de explotación y tarifarios. Y además publica normativa sobre los mismos, con vista a la normalización de las telecomunicaciones a nivel mundial. Con sede en Ginebra (Suiza) fue conocido hasta 1992 como Comité Consultivo Telefónico y Telegráfico (CCITT).

Función Principal: Las normas producidas por el UIT-T son conocidas como "Recomendaciones" (normalmente escrito en mayúsculas para distinguir su significado del sentido ordinario de la palabra recomendación). Dado que el UIT-T es parte la UIT, la cual es un organismo de la Organización de las Naciones Unidas (ONU), sus normas gozan de mayor reconocimiento internacional que las que publican otras organizaciones técnicas en forma similar. [http://www.itu.int/ITUTELECOM/]

[M]

Maestro de Operaciones - FSMO (en inglés *Felxible Single Master Operation*): AD admite la replicación de numerosos maestros del almacén de datos de directorio entre todos los controladores del dominio, de modo que todos ellos se encuentran, básicamente, en el mismo nivel. Esta replicación se la conoce también como “de maestro múltiple” o “multimaster”. Igualmente, hay cambios que no se pueden efectuar empleando la replicación de varios maestros. En esos casos, un controlador de dominio, denominado maestro de operaciones, acepta las solicitudes para realizar este tipo de cambios. En cada bosque existen funciones de maestro de operaciones, propias de los bosques, que se asignan a uno o varios controladores de dominio. Las funciones de maestro de operaciones de todo el bosque deben aparecer una única vez en cada bosque. Existen a su vez funciones de maestro de operaciones a nivel de dominio, las cuales deben aparecer una única vez en cada dominio del bosque. Una explicación con mayor detalle se ha desarrollado en el Paso B4: Determinar la ubicación del Rol de Maestro de Operaciones, en la página 102.

[N]

Nombre Distinguido – DN (en inglés *Distinguished Name*): Todo objeto en AD tiene un DN. En este contexto, distinguido son las cualidades que permiten identificar el nombre. Los nombres distinguidos identifican el dominio que contiene el objeto además del camino completo a través de la jerarquía del contenedor utilizado para alcanzar el objeto.

CN = Se interpreta como nombre propio (*Common Name*)

OU = Unidad Organizacional (*Organizacional Unit*)

DC = significa controlador de dominio (*Domain Controller*)

[K]

KERBEROS: Es un protocolo de autenticación de redes de computadoras creado por el MIT, que permite a dos ordenadores en una red insegura demostrar su identidad de manera segura. Brinda autenticación mutua: tanto cliente como servidor verifican la identidad uno del otro. Los mensajes de autenticación están protegidos para evitar ciertos tipos de ataques como "*eavesdropping"* (escuchar secretamente) y de "*replay"* (ataques de reinyección). Kerberos se basa en criptografía de clave simétrica y requiere un tercero de confianza. Además, existen extensiones del protocolo para poder utilizar criptografía de clave asimétrica. Active Directory emplea el protocolo V5 de Kerberos.

[O]

Objeto de AD: Es un conjunto determinado de atributos que representan algo completo, como puede ser un usuario, una impresora o aplicación. Los atributos contienen la información que describe lo que se identifica por medio del objeto de directorio.

Objetos de Política de Grupo – GPO (en inglés *Group Policy Objects*): Es un conjunto de una o más políticas del sistema. Cada una de estas políticas establece una configuración del objeto al que afecta específicamente. Una directiva de grupo consta de varias componentes configurables. Una son las plantillas administrativas, que definen las directivas basadas en el registro de Windows. Los otros componentes principales son los siguientes:

• Configuración de la seguridad: Configura la seguridad de los usuarios, computadoras y dominios.

• Secuencia de comandos: Especifica las secuencias de comandos para el inicio y el apagado de las computadoras, así como para los eventos de inicio y cierre de sesión de los usuarios.

• Redirección de carpetas: Ubica en la red las carpetas esenciales como mis documentos o las carpetas de aplicación especificada.

• Instalación de Software: Asigna las aplicaciones a los usuarios.

Las GPOs almacenan la información de dos ubicaciones: En una estructura de carpetas denominada plantillas de directiva de grupo (GPT, Group Policy Template) y en un contenedor de directivas de grupo (GPC, Group Policy Container,) de AD. La GPT se halla en la carpeta SYSVOL de todos los controladores de dominio. Contiene información sobre las directivas de software, sobre las distribuciones de archivos y aplicaciones, sobre secuencias de comandos y sobre configuración de seguridad. Las GPC contienen propiedades de las GPO, como la información de clases de AD relacionada con la implantación de las aplicaciones. La información almacenada en las GPC no se modifica con frecuencia.

OCDE: La Organización para la Cooperación y el Desarrollo Económico, es una organización de cooperación internacional, compuesta por 34 estados, cuyo objetivo es coordinar sus políticas económicas y sociales. Fue fundada en 1960 y su sede central se encuentra en el Château de la Muette, en la ciudad de París, Francia. En la OCDE, los representantes de los países miembros se reúnen para intercambiar información y armonizar políticas con el objetivo de maximizar su crecimiento económico y coadyuvar a su desarrollo y al de los países no miembros. Se considera que la OCDE (agrupa a los países más avanzados y desarrollados del planeta, siendo apodada como club de países ricos. Los países miembros son los que proporcionan al mundo el 70% del mercado mundial y representan el 80% del PNB mundial (Producto Nacional Bruto).

OU - Organizacional Unit: Ver Unidad Organizacional

[P]

PROXY: La traducción al español es delegado. Un proxy, en una red informática, es un programa o dispositivo que realiza una acción en representación de otro. Esto es, una hipotética máquina A solicita un recurso a una C, lo hará mediante una petición a B. C entonces no sabrá que la petición procedió originalmente de A. Esta situación estratégica de punto intermedio suele ser aprovechada para soportar una serie de funcionalidades como proporcionar caché (memoria intermedia), control de acceso, registro de tráfico, prohibición de determinado tráfico, por citar algunos. La finalidad habitual es la de servidor proxy, que consiste en interceptar las conexiones de red proveniente de un cliente hacia a un servidor de destino, y operad como intermediario para poder controlar o administrar seguridad, rendimiento, anonimato, entre otros propósitos.

[R]

RAID - Redundant Array of Independent Disks: Ver Conjunto Redundante de Discos Independientes.

Red Privada Virtual – VPN (en inglés *Virtual Private Network*): Denominación que se le da a tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que una computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

[S]

Servicio de Nombres de Internet de Windows – WINS (en inglés *Windows Internet Naming Service*): Es un componente servidor de nombres de Microsoft para NetBIOS, que mantiene una tabla con la correspondencia entre direcciones IP y nombres NetBIOS de ordenadores. Esta lista permite localizar rápidamente a otra computadora en la red. Al usar un servidor de nombres de internet de Windows (WINS) en una red, se evita el realizar búsquedas más laboriosas (como peticiones por difusión) para obtenerla, y se reduce de esta forma el tráfico de la red. A partir de Windows 2000, WINS ha sido relegado en favor del despliegue de los

servicios de DNS y Active Directory. Sin embargo, sigue siendo necesario para establecer servicios de red con versiones anteriores de sistemas operativos Microsoft.

SGR: Las Sociedades de Garantía Recíproca, son entidades financieras cuyo objeto principal consiste en facilitar el acceso al crédito de las pequeñas y medianas empresas (PyMEs) y mejorar, en términos generales, sus condiciones de financiación, a través de la prestación de avales ante bancos, cajas de ahorros y cooperativas de crédito, Administraciones Públicas y clientes y proveedores

Sistema de Archivos Distribuidos – DFS (en inglés *Distributed File System*): Es un sistema de archivos distribuidos o sistema de archivos de red, es un sistema de archivos de computadoras que sirve para compartir recursos como archivos, impresoras y otros como un almacenamiento persistente en una red de computadoras.

Sistema de Nombres de Dominio – DNS (en inglés *Domain Name System*): Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red de computadoras privadas. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente. El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio. AD está fuertemente ligado con el servicio de DNS.

Sitio en AD: En AD, los sitios se definen a través de la agrupación de múltiples subredes físicas. Los sitios suelen ser definidos como ámbitos en los que el acceso a la red informática es altamente fiable, rápido y de costo razonable.

Subsistema Multimedia IP – IMS (en inglés *IP Multimedia Subsystem*): Conjunto de especificaciones que describen la arquitectura de las redes de siguiente generación (*Next Generation Network*, NGN), para soportar telefonía y servicios multimedia a través de IP. Más concretamente, IMS define un marco de trabajo y arquitectura base para tráfico de voz, datos, video, servicios e imágenes conjuntamente a través de infraestructura basada en el ruteo de paquetes a través de direcciones IP. Esto

permite incorporar en una red todo tipo de servicios de voz, multimedia y datos en una plataforma accesible a través de cualquier medio con conexión a internet, ya sea fija, o móvil. Sólo requiere que los equipos utilicen el protocolo de sesión SIP (En inglés *Session Initation Protocol*) que permite la señalización y administración de sesiones.

Éste concepto requiere que cada dispositivo conectado a la red que requiera sesiones multimedia, de voz y de datos, posea una dirección IP única, por lo que la cantidad de direcciones IP necesarias para tener operativa una red de éstas características es mayor al actual soportado por el protocolo IPv4. Por lo mismo IMS requiere la implementación previa del protocolo IPv6, que amplía la cantidad de direcciones IP disponibles para asignar.

[U]

Unidad Organizacional – OU (en inglés *Organizational Unit*): Es una unidad que se define como contenedor de objetos, que se alberga en un dominio. Dentro de esta, puede haber infinidad de objetos que pueden ser usuarios o computadoras. Estas unidades son útiles ya que pueden englobar una cantidad muy grande de objetos dentro de las mismas, permitiendo la organización de objetos dentro del dominio. Simplifica la administración de recursos agrupados. Facilita notablemente la delegación del control de administración. Como concepto de diseño, al crear OU simplifico la aplicación de directivas, permisos y políticas a los recursos reunidos dentro de la misma. Lo anterior es debido a que a este tipo de objetos Contenedores y OUs, son a los únicos que se les puede aplicar las GPOs.

[V]

VPN - Virtual Private Network: Ver Red Privada Virtual

[W]

WINS - Windows Internet Naming Service: Ver Servicio de Nombres de Internet de Windows.

WMI - Windows Management Instrumentation: Ver **I**nstrumentación para la Administración de Windows.

Anexo I

Apéndice: Diseño Ayudas de Trabajo

Estas plantillas permiten definir una base para la documentación de la infraestructura desplegada. (Microsoft, 2008)

1. Cantidad de bosques definidos

   Número ____
   Nombre del Bosque _____

2. Dominios que se han definido por bosque

   Bosque 1____
   …….
   Bosque N____

3. Nombres asignados (DNS y NetBIOS) para cada uno de los dominio (añadir columnas adicionales para los bosques).

Dominio	Bosque 1	Bosque N
1		
2		
3		
N		

4. Lista de dominios raíz para cada bosque.

   Bosque 1_____
   ……
   Bosque N_____

5. Diseño de las Unidades Organizativas para cada dominio.

OU nombre	Dominio	Propósito	Controles

6. Determinar la ubicación del controlador de dominio para cada dominio.
    a. Esbozar la ubicación física del controlador de dominio.

7. Determinar el número de controladores de dominio para cada ubicación.

Ubicación	Número de controladores de dominio de

8. Plan global de ubicación de servidores de catálogo para cada bosque.
    a. Esbozar la ubicación de servidor de catálogo global.

9. Plan de la ubicación de la función FSMO de cada bosque y dominio.
    a. Esbozar la ubicación de FSMO.

10. Crear el diseño de los sitios.
    a. Esbozar el diseño del sitio.

11. Crear el diseño de vínculos de sitios.
    a. Esbozar el diseño de vínculos de sitios.

12. Establecer el diseño de los servidores físicos.

Nombre de servidor	CPU	Tamaño de discos / configuración	Memoria