UNIVERSIDAD NACIONAL DE LA PLATA

FACULTAD DE INFORMÁTICA

TESINA DE LICENCIATURA

Título: "Integración de servicios de autenticación en una Organización gubernamental con alcance Nacional. Caso de estudio e Implementación."
Autor: Foster, Pablo Mauricio
Director: Marrone, Luis
Codirector: --
Asesor profesional: Bilbao, Héctor
Carrera: Licenciatura en Sistemas

Resumen

El presente trabajo hace foco en la problemática relacionada a la validación de credenciales de usuarios, presente en un organismo gubernamental. Se describe la infraestructura informática inicial de dicho organismo haciendo hincapié en las componentes que conforman tanto la red, como los servicios/aplicaciones que son los principales focos dentro del análisis realizado y descripto.
Presenta las distintas alternativas para lograr que cada una de las partes de dicha infraestructura funcione como una unidad compacta y no como partes con una pobre interacción entre sí. La intención es simplificar y optimizar principalmente los procesos relacionados a la autenticación para hacer uso de los recursos relacionados con la información. Como producto final, se ofrece una visión consolidada de dicho organismo cuya principal mejora se basa en la unificación de diversas fuentes de información relacionada con credenciales de acceso (usuario/clave) logrando contar con un único repositorio contra el cual se puedan realizar las operaciones de autenticación.
Todo el análisis y planteo se realiza en base a las realidades del Organismo evaluado, y con la premisa de minimizar el impacto sobre el normal funcionamiento de la infraestructura del mismo.

Palabras Claves

Autenticación, usuario, clave, LDAP, integración, Active Directory, replicación, servicios, información, infraestructura

Conclusiones

El estudio reflejado en el presente trabajo, ha permitido definir los lineamientos para la expansión de la infraestructura informática relacionada con los procesos de validación de usuarios para el acceso a la información. Ha permitido unificar diversas fuentes de información, logrando una convergencia que facilitará futuras implementaciones.

Trabajos Realizados

Análisis de situación y problemáticas. Estudio de soluciones a problemas similares en el mercado. Selección de solución en base a las distintas variables que se conjugan en el ámbito de aplicación particular.

Trabajos Futuros

Continuar con la expansión de la infraestructura informática descripta en el presente trabajo, con el resto de las oficinas que forman parte del Organismo analizado. A su vez, introducir nuevos mecanismos que permitan agilizar los procesos de autenticación entre distintos organismos del Estado como el que se describe. Promulgar la inversión en tecnología relacionada a la información, de manera de poder involucrar nuevos procesos como ser firma digital, introducción de mecanismos de autenticación a través de OAuth.

Fecha de la presentación: Noviembre 2012

2012

Integración de servicios de autenticación en una Organización gubernamental con alcance Nacional. Caso de estudio e Implementación.

Facultad de Informática

Universidad Nacional de La Plata

A.C. Mauricio Foster

Trabajo de Grado

Contenido

Índice de Figuras **5**

1. Objetivos **6**

1.1 Motivación 6

1.2 Pasos a seguir 6

1.3 Introducción 7

1.4 Estructura Organizativa del trabajo 9

2. Resumen **10**

3. Servicios de Directorio LDAP (Introducción) **12**

3.1 Directorios 13

3.1.1 Directorio VS bases de datos relacionales 14

3.1.2 LDAP: Protocolo o directorio 16

3.1.3 Directorios distribuidos 17

3.2 Ventajas del uso de un directorio 18

3.3 Historia de LDAP y los estándares 20

3.3.1 OSI e Internet 20

3.3.2 Estándar de servidor de Directorio X.500 21

3.4 Estructura 23

3.4.1 La estructura de un árbol de directorio LDAP 23

3.4.2 Personalización de clases 25

3.5 Ejemplo de una entrada individual LDAP 27

4. Descripción del entorno **29**

4.1 ¿Qué es y qué hace Senasa? 29

4.2 Situación Inicial 31

4.2.1 Infraestructura de red del Organismo 33

4.2.2 Infraestructura de Servicios 36

5. Desarrollo **44**

¿Qué problemas se desean resolver? (“Conjunto de partes” VS “Partes de un todo”) 44

5.1 Punto 1: Visión disgregada del Organismo 45

5.1.1 Alternativas de solución 47

5.1.2 Selección de alternativa: propuesta de solución 56
5.2 Punto 2: Dos grandes repositorios de usuarios disjuntos 63
5.2.1 Alternativas de solución 65
5.2.2 Selección de alternativa: propuesta de solución 70
6. Beneficios obtenidos 84
6.1 Desde el punto de vista de la administración 85
6.2 Desde el punto de vista de la seguridad 86
6.3 Desde el punto de vista de la visión unificada de la organización 87
6.4 ¿Qué sucede con las dependencias de tipo 2? 88
7. Conclusiones 89
7.1 Aspectos destacados 89
7.2 Situación a la fecha 90
7.3 ¿Dónde es aplicable esta solución? 90
7.4 A futuro 91
Anexos 92
Anexo I: Active Directory Services (ADS) 92
Estructura 92
Objetos 93
Funcionamiento 93
Anexo II: Active Directory Lightweight Directory Service (AD LDS) 94
¿Qué hace AD LDS? 94
Glosario 95
Referencias 101

Índice de Figuras

Figura 1: Ejemplo de directorio LDAP 29

Figura 2: Centros Regionales en Argentina 31

Figura 3: *Situación Actual para Centros Regionales, Oficinas principales, Laboratorios, y Estación de Cuarentena (Dependencias Tipo 1)* 35

Figura 4: Situación Actual para Oficinas locales, Puertos, aeropuertos y otros pasos de frontera (Dependencias Tipo 2) 36

Figura 5: En Central, dos Servicios de Directorio me permiten acceder a distintos recursos de la red 39

Figura 6: Servicio de directorio de LDAP con alcance para todo el país 39

Figura 7: Open LDAP como repositorio de credenciales de usuario en todo el país 49

Figura 8: Dominio único en todo el país 52

Figura 9: Dominio principal y subdominios 54

Figura 10: Dominios independientes relacionados a través de "confianza" 55

Figura 11: Configuración de cada dependencia de tipo 1 62

Figura 12: El usuario cambia su clave desde una aplicación ó servicio autenticado en LDAP 66

Figura 13: El usuario cambia su clave desde una aplicación ó servicio autenticado en Active Directory 66

Figura 14: Solución a través de un metadirectorio. 68

Figura 15: Unificar las bases de datos de usuarios empleando Active Directory 69

Figura 16: Estructura de la solución propuesta a través de la herramienta AD LDS. 72

Figura 17: Ejemplo de un usuario proxy 74

Figura 18: Base de datos de AD LDS 75

Figura 19: Verificación de datos cuando el usuario está dentro de ADS senasa 77

Figura 20: Verificación de datos cuando el usuario está dentro de LDAP-AD LDS 78

Figura 21: La base de datos del AD LDS sólo en Casa Central 80

Figura 22: La base de datos del AD LDS en cada dependencia de tipo 1 81

Figura 23: Las aplicaciones se conectan de manera directa a la base de datos de usuarios 83

Figura 24: Capa de abstracción entre las aplicaciones y la base de datos de usuarios 84

1. Objetivos

El objetivo del presente trabajo es describir el desarrollo de un proyecto real que pretende la evolución de la manera en la que los agentes de un Organismo gubernamental, validan sus credenciales de usuario para hacer uso de los recursos de dicho Organismo dentro de una red con alcance en toda la República Argentina.

A su vez, intenta modificar la visión disgregada que se tiene del Organismo desde el punto de vista tecnológico, al contar con varias fuentes disjuntas de información y con escasa relación entre sí, por una visión unificada y consolidada del mismo.

Este desarrollo se inicia con los primeros análisis, aquellos que permiten detectar las necesidades dentro de los procesos antes mencionados, pasando por la evaluación de cada una de las alternativas de solución hasta la selección de una de ellas, brindando por último los detalles correspondientes a los procesos involucrados en su implementación.

1.1 Motivación

El número de sistemas informáticos en las organizaciones medianas y grandes se encuentra en continuo crecimiento, por lo que la gestión de usuarios se ha convertido en uno de los problemas más relevantes en este tipo de organizaciones. A su vez, los mismos usuarios con diferentes roles acceden a diferentes aplicaciones o servicios, por lo que la demanda de contar con un único par usuario/clave para acceder a las aplicaciones va en un sostenido aumento y es una necesidad que debe atenderse.

1.2 Pasos a seguir

- Análisis de la situación actual
    - Problemas encontrados
- Enumeración de alternativas de solución
    - Ventajas y desventajas de cada una
- Implementación de la solución
    - ¿Nuevos problemas?

1.3 Introducción

En cualquier organización de mediano o gran tamaño, basta hacer un pequeño paneo para detectar que el número de sistemas informáticos no sólo se encuentra en continuo crecimiento, sino que en algunos casos se convierte en un problema en sí mismo por motivos principalmente relacionados a la administración de recursos tales como usuarios, claves y roles. Esto es debido a la enorme matriz que se presenta combinando por un lado las aplicaciones/servicios existentes, los usuarios y nivel de acceso ó roles que cada uno de esos usuarios cuenta para cada uno de los aplicaciones/servicios en cuestión.

Si a la matriz anterior, le sumamos la complicación adicional que los repositorios desde donde se toman los usuarios a ser validados, suele no ser una única fuente uniforme y homogénea, sino por el contrario puede tratarse de diversas fuentes de datos, la complejidad crece más aún y de una manera abrumadora.

El presente trabajo se inicia como el resultado de la búsqueda de soluciones integrales para varias falencias encontradas en la infraestructura informática de un organismo nacional con recursos asociados a la información dispersos en todo nuestro país. Dichas falencias suelen hacer que problemas de tipo diario, se tornen enormes y por momentos hasta inmanejables debido a factores como la cantidad de recursos comprometidos, y por la carencia de herramientas precisas para encontrar y/ó solucionar los mismos en tiempos razonables.

Para los tiempos que corren, un administrador de infraestructura de redes y servicios, como es mi caso, se vale 100% no sólo de su conocimiento, de vivencias anteriores, sino también de las herramientas tecnológicas con las que cuenta. Serán estas últimas los “ojos” que le permitan a uno tener un diagnóstico preciso del estado de situación ante un problema. Podríamos afirmar sin riesgo a equivocarnos, que el mejor de los administradores de servicios, poco podría hacer ante cualquier problema normal que pudiera suceder en un día común de trabajo, sin las herramientas necesarias. De igual manera que le sucede al mejor y más exquisito de los carpinteros (sólo por citar una profesión que ejemplifique), quien se encontraría imposibilitado de confeccionar sus mejores trabajos en caso de no contar con sus tan preciadas herramientas.

El mundo de TI (*Tecnología de la Información*) no es una excepción a esta regla. Todos nos valemos de las herramientas existentes para poder tener más precisión, para poder realizar más tareas en menos tiempo, para poder mantener más equipos en estado funcional durante períodos más prolongados, en fin, para cada una de las pequeñas tareas que llevamos a cabo de manera rutinaria. Y es precisamente dicha herramienta la que nos permitirá controlar con mayor o menor precisión las situaciones que tengamos que enfrentar a lo largo de nuestra carrera profesional.

Sin embargo, muchas veces la elección de dicha herramienta suele ser por sí misma, una tarea por demás compleja en la que se ven involucrados un gran número de factores de todo tipo y en muchas ocasiones, un gran número de personas con roles e intereses muy distintos dentro de la misma organización. Desde personal contable, desarrolladores, administradores de red y

servicios, soporte técnico, comunicaciones, etc. Esta heterogeneidad de perfiles, suele complicar aún más el proceso de selección de una herramienta. Otros factores que suelen tener una incidencia directa sobre el proceso de selección de la herramienta (y sólo para citar algunos) pueden ser:

- La política de la organización.
- Razones de tipo económica o financiera.
- Razones de disponibilidad del producto en el área geográfica donde se lo requiere.
- Disponibilidad o no de recursos de hardware para su implementación, y la posibilidad o no de adquirirlos.
- Disponibilidad o no de recursos humanos para su implementación, y la posibilidad o no de adquirirlos.
- Preconceptos hacia la herramienta por alguna razón, como por ejemplo una mala experiencia previa.
- Complejidad de la solución.
- Tiempos requeridos en la provisión de las herramientas por parte de los proveedores.
- Tiempos esperados en la implementación de la solución.

A todo esto debemos agregar que una solución debe ser pensada y concebida para ser mantenida en el tiempo. Es decir, que los factores que posibilitan su implementación deben ser analizados durante el tiempo sobre el que se espera se mantenga la solución. Y es aquí cuando muchas de las soluciones “ideales” suelen perder fuerza, dado que en algunas situaciones, las mismas no son fáciles de mantener en el tiempo. Ya sea por costos de mantenimiento, recursos humanos, complejidad o algún otro factor de los previamente mencionados.

Este trabajo intentará analizar en detalle las principales debilidades de la infraestructura informática del organismo para así aprender de ellas, para lograr entender qué es lo que se desea abordar y tratando de evitar perder el foco del problema con las bifurcaciones que podrían llegar a surgir.

A modo introductorio diremos que la principal falencia tiene que ver con una visión disgregada presente en el organismo. Es decir que a simple vista, podríamos decir que se encuentra compuesto por varios sub-organismos independientes que a su vez cuentan con una infraestructura informática independiente del resto (servicios, redes, usuarios, etc), sólo unidas por un vínculo de comunicaciones a través del cual no se pueden establecer parámetros comunes a las mismas. De hecho, cualquiera podría decir que dichas redes no forman parte de UN organismo, sino que son una sumatoria de recursos dispersos con poca relación entre sí. Esta estructura es la consecuencia de muchos factores, pero principalmente está relacionado con el gran y rápido crecimiento que ha tenido la organización en cuanto a dispersión geográfica, recursos humanos, información, procesos, en algunos casos sin el debido acompañamiento de un crecimiento tecnológico acorde.

En resumen, podemos decir que el organismo está compuesto por varias partes con poca relación entre sí lo cual dificulta la visión de la infraestructura como una unidad. A su vez, se

intentará mostrar cómo algunas de las actividades diarias que se realizan desde el Senasa [1] (organismo foco del desarrollo), podrían verse facilitadas en gran medida, a partir de la concepción de todas las redes distribuidas geográficamente en nuestro país, como un todo, como una unidad organizacional bajo una misma administración.

A través de la infraestructura informática que el organismo posee, se brindan diversos servicios tanto de manera interna como también hacia muchos otros organismos o entidades, ya sean dependientes de Senasa o externos a este, dispersos geográficamente en el mapa de la República Argentina. Por tal motivo, y teniendo en cuenta el nivel de compromiso que una entidad de tamaña envergadura posee, se procede con diversos análisis como el que se presenta en este documento enfocándonos en mejorar las soluciones ofrecidas, facilitando además, futuras implementaciones que pudieran llegar a necesitar convivir con las existentes al día de hoy.

Como sucede en muchas organizaciones no sólo públicas, sino también dentro del ámbito privado, la necesidad imperiosa de contar en forma rápida con nuevos servicios relacionados a la informática y sumado a la creciente complejidad de los mismos, llevan a no detenernos en exhaustivos análisis para determinar la “mejor” manera de adaptar la infraestructura existente a los nuevos requerimientos. A esto hay que sumarle la carencia de recursos humanos y presupuesto para iniciar proyectos que acompañen con la verdadera envergadura de los proyectos. Sin duda esto debería ser uno de los pasos a seguir para lograr que la convivencia entre lo que existe y los nuevos desarrollos/servicios conformen una solución óptima, pero lamentablemente y por razones que exceden al análisis planteado en este documento no serán planteados, esto no siempre es así. Esto lleva a que las nuevas implementaciones se adecuen a la infraestructura existente “como se puede”, encajando como piezas de diferentes rompecabezas trayendo como consecuencia en algunos casos, que viejas malas prácticas ya instaladas se propaguen en el tiempo.

Es decir, que las infraestructuras crecen en forma rápida, pero no siempre eficiente, eficaz y/ó simple. Es por ello que, a través del presente documento se ofrece un análisis más detallado de la situación inicial de la infraestructura tecnológica correspondiente a la organización Senasa, de manera de tener las herramientas necesarias para realizar una propuesta a través de la cual se pueda evaluar una configuración alternativa, en donde se integren de manera más funcional todos los elementos que existen permitiendo que los mismos puedan interactuar más eficientemente.

1.4 Estructura Organizativa del trabajo

La presente tesis de grado está compuesta por 7 (siete) capítulos que enmarcan tanto las partes de análisis, propuesta y desarrollo de la solución implementada así como también la conclusión y resultados obtenidos.

A través del capítulo 2 se introduce al lector en la problemática desarrollada en el presente trabajo mediante un resumen de la misma, en el cual se brinda una introducción de los aspectos analizados en cada caso.

A través del capítulo 3, se lleva a cabo una introducción teórica de uno de los principales conceptos que se analizarán a lo largo del resto del trabajo, y que permitirá contar con más y mejor información a la hora de realizar análisis y justificar algunas de las elecciones realizadas. El concepto en cuestión, coincide con el nombre del capítulo y es "Servicios de Directorio LDAP".

El capítulo 4, de nombre "Descripción del Entorno", describe cómo está conformado el entorno sobre el cual se desarrolla el presente trabajo. La cobertura de dicho entorno está dada por una descripción mínima de lo que hace Senasa, su división estratégica y su rol dentro de la sociedad. También se describen aspectos más técnicos relacionados con la infraestructura del Organismo tanto a nivel de red, como de servicios, de manera de poder entender más fácilmente muchos de los análisis llevados a cabo en el presente trabajo.

En el capítulo 5 se inicia la descripción del desarrollo propiamente dicho de la solución. Por tal razón se trata del capítulo con mayor contenido técnico dentro del trabajo. En primer medida, se hace una introducción de cada uno de los problemas a resolver, posteriormente se introducen todas las alternativas posibles de solución para luego mostrar la alternativa seleccionada, razones, ventajas y desventajas.

En el capítulo 6 se introducen en detalle todos los beneficios que se obtuvieron a partir de la implementación previamente analizada. Estos beneficios se tipifican de una manera particular, teniendo en cuenta distintos puntos de vista.

Por último, en el capítulo 7 se ofrecen las conclusiones obtenidas en base al análisis y a la implementación de la solución.

Cabe destacar que al final del trabajo, el lector cuenta con una sección de *Anexos* en donde podrá obtener información acerca de algunos de los productos de software mencionados en el presente. Luego se brinda otra sección de nombre *Glosario* en donde se puede obtener el significado de algunas palabras técnicas empleadas durante el documento y por último la sección *Referencias* en donde listan las fuentes de información empleadas para el estudio.

2. Resumen

Como objetivo principal, el presente trabajo describe la infraestructura informática inicial del organismo e introduce la problemática que lleva a la decisión de realizar modificaciones sustanciales sobre la misma. Dicha descripción se realiza haciendo hincapié en las componentes

que conforman tanto la red, como los servicios/aplicaciones que son los principales focos dentro del análisis realizado y descripto en el presente documento.

Presenta las distintas alternativas para lograr que dicha infraestructura pueda funcionar como una unidad organizacional, entendiendo por ello, una red bajo una misma administración en la cual el hecho de compartir recursos (aplicaciones, usuarios, bases de datos, configuraciones, información en general, etc) a lo largo de la red distribuida en el país, pueda lograrse de manera natural y eficiente y no implique que en algunos casos, dichos recursos deban ser definidos de manera repetida en más de una ubicación. De esta manera, se logra no sólo simplificar en gran medida tareas tales como la administración de los recursos, sino también evitar duplicidad de información u objetos a lo largo del organismo, facilitando operaciones que involucran a muchos equipos de red y muchas horas de recursos humanos.

El análisis está enfocado a los repositorios de la información relacionada a credenciales de usuarios empleadas para autenticarse, la manera en que los mismos se distribuyen geográficamente en la infraestructura informática, y a la forma en que cada una de estas componentes de red e información interactúa con el resto.

Se evalúan las complicaciones generadas por no contar con un repositorio único y centralizado de credenciales, en donde se encuentre toda la información relacionada tanto a las personas que pudieran llegar a tener acceso a la información del organismo, como también al nivel de acceso que las mismas cuentan sobre dichos recursos. Luego, y en base a lo anterior, se brindan diferentes opciones de solución que se presentan con las bondades y desventajas de cada una de ellas.

La intención es lograr determinar las modificaciones a llevar a cabo en la infraestructura informática que sirve de sustento para los servicios prestados desde Senasa de manera tal de lograr una visión consolidada de la organización a nivel funcional y corporativo, en lugar de verlo como varias dependencias independientes unidas por vínculos de red.

La principal motivación de este trabajo es la posibilidad de poder plasmar en un organismo real, en una infraestructura existente la solución que mejor se adecua a las necesidades de una organización modelo de la República Argentina con todo el análisis previo que lo antecede. Se evalúan las posibles soluciones, analizando cada uno de los riesgos que introducidos por cada una de ellas, y haciendo hincapié en las virtudes y problemas que surgieran de las decisiones tomadas.

Esto nos permitirá darnos cuenta dónde estamos parados a nivel de arquitectura de TI, y hasta dónde un organismo estatal como el analizado, con necesidades, realidades, y posibilidades de un organismo estatal puede adecuarse a las soluciones que ofrecen las mejores prácticas a nivel mundial.

Luego, y en base a dicho análisis, se proponen una serie de opciones posibles de manera tal que, a través de las modificaciones que las mismas implican, se logran mejoras significativas en

pos de un funcionamiento más integrado y unificado, sin que ello implique a su vez una inversión significativa en términos económicos.

3. Servicios de Directorio LDAP (Introducción)

Lightweight Directory Access Protocol (LDAP) es una tecnología en creciente expansión que permite el acceso a la información de un directorio. Se trata de un estándar abierto e independiente del proveedor/infraestructura que proporciona una arquitectura extensible para el almacenamiento centralizado y gestión de la información que debe estar disponible para cualquier sistema ó servicio distribuido actual.

Después de un inicio rápido, LDAP se ha convertido en el método de acceso por defecto a la información de directorios, comparable con el sistema de nombres de dominio (DNS) [2] el cual se emplea para buscar una dirección IP a partir de un nombre (y viceversa) en casi todos los sistemas y redes independientemente de su tamaño (intranets/Internet). En la actualidad, LDAP es soportado por la mayoría de los sistemas operativos y aplicaciones, incluso aquellas más cerradas.

Hoy la gente y las empresas confían en los sistemas informáticos para soportar las aplicaciones distribuidas las cuales pueden interactuar tanto con equipos de la misma red de área local (LAN), dentro de una intranet corporativa, dentro de extranets conectadas con socios y proveedores, o en cualquier parte del mundo a través de Internet. Para mejorar la funcionalidad y la facilidad de uso, y para permitir una administración con un costo aceptable de las aplicaciones distribuidas, toda la información relacionada a servicios, recursos, usuarios y demás objetos accesibles desde las aplicaciones debe ser organizada de una manera clara y coherente. Mucha de esta información puede ser compartida entre varias aplicaciones, por tal motivo la misma debe ser protegida con el fin de evitar la modificación no autorizada o la divulgación de información privada.

La información que describe los diversos usuarios, aplicaciones, archivos, impresoras y otros recursos accesibles desde una red a menudo se recoge en una base de datos especial que a veces se la llama directorio. Dado el crecimiento en el número de redes y aplicaciones, el número de directorios de información especializados también ha crecido, lo que resulta en islas de información difíciles de compartir y gestionar. Si toda esta información pudiera ser mantenida y accedida de una manera consistente y controlada, proporcionaría un punto neurálgico para la integración de un entorno distribuido en un sistema coherente y uniforme.

El protocolo LDAP es un estándar abierto de la industria que ha evolucionado para satisfacer estas necesidades. LDAP define un método estándar para acceder y actualizar la información en un directorio y ha ganado amplia aceptación como método de acceso de directorio

en Internet convirtiéndose en estratégico dentro de intranets corporativas. A su vez, es soportado por un creciente número de proveedores de software y está siendo incorporado en un número creciente de aplicaciones.

3.1 Directorios

Un directorio es un listado de la información detallada de objetos dispuestos en un orden particular. Los ejemplos más comunes son un directorio telefónico (guía) y un catálogo de una biblioteca. Para el caso de un directorio telefónico, la lista de objetos estaría dada por las personas en donde los nombres están ordenados alfabéticamente, y los datos proporcionados sobre cada persona son mínimamente su dirección y su número telefónico.

En el caso del catálogo de una biblioteca, los libros están ordenados por autor ó por título, y también se podría brindar información adicional como ser el número ISBN u otra información de publicación.

En términos informáticos, un directorio es una base de datos especializada, también llamada repositorio de datos, que almacena y ordena información tipificada acerca de objetos. Un directorio particular podría, por ejemplo, contener información tipificada de impresoras (los objetos) como ser la ubicación (una cadena de caracteres con formato), la velocidad en páginas por minuto (numérico), flujos de impresión compatibles (por ejemplo, PostScript o ASCII) entre otros datos.

Los directorios permiten a los usuarios y a las aplicaciones encontrar recursos con características particulares para una tarea particular. Por ejemplo, un directorio de usuarios podría ser empleado para buscar el correo electrónico ó número de fax de alguien particular. El directorio de impresoras, podría ser empleado para buscar la impresora PostScript color más cercana a una determinada ubicación. O un directorio de aplicaciones podría ser empleado para encontrar un servidor que pudiera contener información sobre la facturación de clientes.

Los términos de páginas blancas y páginas amarillas se utilizan a veces para describir cómo un directorio se utiliza. Si el nombre de un objeto (persona, impresora) es conocido, sus características (número de teléfono, páginas por minuto) pueden ser recuperadas fácilmente de igual manera que se busca un nombre en las páginas blancas de la guía telefónica. Si el nombre de un objeto individual particular no se conoce, el directorio puede ser empleado para buscar una lista de los objetos que cumplen un requisito determinado, de manera similar a como se busca una lista de pizzerías en las páginas amarillas de la guía telefónica. Sin embargo, los “directorios informáticos” son mucho más flexibles que las páginas amarillas de un directorio telefónico, ya que por lo general permiten búsquedas por criterios específicos, no sólo por un conjunto predefinido de categorías.

3.1.1 Directorio VS bases de datos relacionales

Un directorio se describe a menudo como una base de datos, pero se trata de una base de datos especializada que tiene características que lo diferencian de las bases de datos relacionales de propósito general. Una característica especial de los directorios es que son accedidas (para leer o realizar búsquedas) mucho más a menudo de lo que se actualizan (accesos de escritura). Cientos de personas puede buscar el número de teléfono de una persona, o miles de clientes de impresión podrían consultar las características de una determinada impresora, pero el número de teléfono o una característica de un impresora rara vez cambian.

Dado que los directorios deben ser capaces de soportar grandes volúmenes de peticiones de lectura, los mismos se encuentran optimizados para ese tipo de acceso. El acceso de escritura puede ser limitado a los administradores del sistema o al propietario de cada pieza de información. A diferencia de esto, las bases de datos relacionales de propósito general brindan sustento a aplicaciones (tales como reservas aéreas, bancarias) en las cuales se llevan a cabo un gran número de actualizaciones sobre los datos.

Debido a que los directorios están diseñados y optimizados para almacenar información relativamente estática, es que no son apropiados para almacenar información que cambie frecuentemente. Por ejemplo, el número de tareas actualmente encoladas en una cola de impresión, probablemente no deba ser almacenado en una entrada de directorio para una impresora, dado que dicha información tendría que ser actualizada con frecuencia. En su lugar, la entrada de directorio para la impresora puede contener la dirección de red de un servidor de impresión. El servidor de impresión se puede consultar para obtener la longitud actual de la cola de impresión si así se deseara. La información en el directorio (la dirección del servidor de impresión) es estática, mientras que el número de tareas en la cola de impresión es dinámico.

Otra diferencia entre los directorios y las bases de datos relacionales de propósito general, es que la mayoría de las implementaciones de directorio aún no soportan transacciones. Las transacciones son operaciones tipo “todo o nada” en donde o bien se completa la totalidad de la misma, o no se ejecuta nada. No sirve que sólo se complete una parcialidad de la operación. Por ejemplo, cuando se efectúa una transferencia de dinero desde una cuenta bancaria a otra, el dinero debe ser debitado de una cuenta y acreditado en la otra cuenta en una sola transacción. Si sólo la mitad de esta transacción se completara, o alguien accediera a las cuentas mientras que el dinero está en tránsito, no tendríamos un balance correcto de dichas cuentas. Las bases de datos relacionales de propósito generalmente brindan soporte para estas transacciones.

A su vez, y debido a que las bases de datos relacionales de propósito general deben dar soporte a aplicaciones de tipo bancarias, de control de inventario entre otras tantas, permiten almacenar colecciones de datos arbitrarios. Los directorios pueden ser limitados respecto al tipo de datos que permiten almacenar (aunque la arquitectura no impone tal limitación). Por ejemplo,

un directorio especializado para la información de contacto de clientes, podría limitarse a almacenar sólo información personal, como nombres, direcciones y números de teléfono. Si un directorio es extensible, podría ser configurado para almacenar una variedad de tipos de información lo que lo hace más útil para una variedad de programas.

Otra diferencia importante entre un directorio y una base de datos relacional de propósito general, es la forma en que la información puede ser accedida. La mayoría de las bases de datos soportan un método estandarizado, un acceso muy poderoso llamado *Lenguaje de Consulta Estructurado* (SQL) [1]. SQL permite actualizaciones y consultas complejas que pueden ser empleadas en aplicaciones de gran tamaño y complejidad. Por otro lado, los directorios tales como un directorio LDAP, utilizan un protocolo de acceso simplificado y optimizado que puede ser utilizado en aplicaciones livianas y relativamente simples.

Como los directorios no están destinados a proporcionar funciones como las proporcionadas por las bases de datos relacionales de propósito general, pueden ser optimizados para brindar a las aplicaciones acceso rápido a los datos de directorio en grandes ambientes distribuidos de una manera más sencilla y económica. Si el uso previsto del directorio es de lectura, es decir, en un ambiente no transaccional, entonces tanto el cliente como el servidor de directorio pueden ser simplificados y optimizados.

Dentro de esta arquitectura de tipo cliente/servidor, las solicitudes son realizadas típicamente por los clientes de directorios, y el proceso que realiza la búsqueda de información dentro del mismo es el servidor de directorio. En general, los servidores proporcionan un servicio específico a los clientes y un servidor podría convertirse en el cliente de otros servidores con el fin de recabar la información necesaria para procesar una solicitud.

Una API [2] define la interfaz de programación que un lenguaje de programación en particular utiliza para acceder a un servicio. El formato y contenido de los mensajes intercambiados entre el cliente y el servidor deben adherirse a un protocolo acordado.

En resumen y para resaltar las diferencias aquí descriptas se listan a continuación las características más importantes que diferencian un directorio LDAP de una base de datos relacional de propósito general:

- Con respecto a las ***bases de datos relacionales***:

    1. Realizan operaciones de escritura intensivas: están preparadas para hacer un uso constante de operaciones orientadas a transacciones, que implican la modificación o borrado constante de los datos almacenados.
    2. Esquema específico para cada aplicación: son creadas para cada aplicación específica, siendo complicado adaptar los esquemas a nuevas aplicaciones.

[1] *Ver **Glosario** al final del documento*
[2] *Ver **Glosario** al final del documento*

3. Modelo de datos complejo: permiten manejar complejos modelos de datos que requieren muchas tablas, foreign keys[3], operaciones de unión (join [4]) complejas, etc.
4. Integridad de datos: todos sus componentes están desarrollados para mantener la consistencia de la información en todo momento. Esto incluye operaciones de rollback[5], integridad referencial y operaciones orientadas a transacciones.
5. Las transacciones se efectúan siempre aisladas de otras transacciones. De tal forma que si dos transacciones *A* y *B* están ejecutándose de forma concurrente los efectos de la transacción *A* son invisibles a la transacción *B* y viceversa, hasta que ambas hayan sido completadas.
6. Disponen de operaciones de rollback (vuelta atrás). Hasta el final de la transacción ninguna de las acciones llevadas a cabo pasa a un estado final. Si el sistema falla antes de finalizar una transacción, todos los cambios realizados son eliminados (rollback)

- Las características de un ***servidor de directorio LDAP*** son:

1. Operaciones de lectura muy rápidas. Debido a la naturaleza de los datos almacenados en los directorios las lecturas son más comunes que las escrituras.
2. Datos relativamente estáticos. Los datos almacenados en los directorios no suelen actualizarse con mucha frecuencia.
3. Entorno distribuido, fácil replicación.
4. Estructura jerárquica. Los directorios almacenan la información de forma jerárquica de forma nativa.
5. Orientadas a objetos. El directorio representa a elementos y a objetos. Los objetos son creados como entradas, que representan a una colección de atributos.
6. Esquema estándar. Los directorios utilizan un sistema estándar que pueden usar fácilmente diversas aplicaciones.
7. Atributos multi-valor. Los atributos pueden almacenar un valor único o varios.
8. Replicación multi-master. Muchos de los servidores LDAP permiten que se realicen escrituras o actualizaciones en múltiples servidores.

3.1.2 LDAP: Protocolo o directorio

Lightweight Directory Access Protocol (LDAP) define un protocolo de mensajes utilizado por los clientes y los servidores de directorio LDAP. El protocolo utiliza diferentes mensajes. Por

[3] *Ver **Glosario** al final del documento*
[4] *Ver **Glosario** al final del documento*
[5] *Ver **Glosario** al final del documento*

ejemplo, un ***bindRequest*** [6] puede ser enviado desde el cliente al servidor LDAP al comienzo de una conexión. Un ***SearchRequest*** [7]se utiliza para buscar una entrada específica en el directorio.

También hay APIs asociadas a LDAP para los distintos lenguajes de programación que permiten acceder a LDAP desde las aplicaciones. En general con LDAP, el cliente no depende de una aplicación particular del servidor.

LDAP es un estándar abierto que define un método para acceder a y actualizar la información en un directorio. LDAP ha ganado amplia aceptación como el método de acceso a directorio de Internet y se está convirtiendo también en estratégico dentro de redes corporativas. Está siendo soportado por un número cada vez mayor de proveedores de software y se está incorporando a un número cada vez mayor de aplicaciones.

LDAP define un protocolo de comunicación. Es decir, se define el transporte y formato de los mensajes utilizados por un cliente para acceder a los datos en un directorio tipo X.500 [3] LDAP no define el servicio de directorio en sí. Cuando se habla de un directorio LDAP, nos referimos a la información que está almacenada y puede ser recuperada por el Protocolo LDAP.

Todos los servidores de directorio LDAP modernos están basados en la versión 3 de LDAP. Se puede utilizar la versión 2 del cliente con un servidor de la versión 3. Sin embargo, no se puede utilizar una versión 3 cliente con un servidor de la Versión 2 a menos que se realice el bind entre los mismos como una versión 2 del cliente y utilizar sólo APIs versión 2.

Todos los servidores LDAP comparten muchas características básicas ya que se basan en el modelo de RFC (*Request for Comments*)[8]. Sin embargo, y debido a diferencias de implementación, no todos son totalmente compatibles entre sí cuando no hay un estándar definido.

3.1.3 Directorios distribuidos

Los términos *local*, *global*, *centralizado* y *distribuidos* se utilizan a menudo para describir un directorio. Estos términos significan cosas diferentes en diferentes contextos. En esta sección, se explica cómo estos términos se aplican a los directorios.

En general, local significa “cerca”, y global que se propaga a través del universo de interés. El universo de interés puede ser una empresa, un país, o todo el mundo. Local y global son dos extremos de un continuo. Esto es, algo puede ser más o menos global o local que otra cosa. Centralizado significa que algo está en un lugar, y distribuido que algo está en más de un lugar. Al igual que con local y global, algo puede ser distribuido en mayor o menor medida.

[6] *Ver **Glosario** al final del documento*
[7] *Ver **Glosario** al final del documento*
[8] *Ver **Glosario** al final del documento*

La información almacenada en un directorio puede ser a la vez local y global en cuanto a su ámbito de aplicación. Por ejemplo, un directorio que almacena la información de manera local podría contener los nombres, direcciones de correo electrónico, y demás información de los miembros de un departamento o grupo de trabajo. Un directorio que almacena información en forma global puede almacenar información para toda una empresa. Aquí, el universo de interés es la empresa.

Los clientes que acceden a la información en el directorio pueden ser locales o remotos. Los clientes locales pueden estar situados en el mismo edificio ó en la misma LAN. Los clientes remotos pueden estar distribuidos por todo el continente o el mundo.

El directorio en sí mismo puede ser centralizado o distribuido. Si un directorio está centralizado, puede haber un servidor de directorio en un lugar o un servidor de directorio que almacena datos de los sistemas distribuidos. Si el directorio se distribuye, hay múltiples servidores, por lo general dispersos geográficamente, que proporcionan acceso a los datos.

Cuando un directorio está distribuido, la información almacenada en él puede estar en particiones o replicada. Cuando la información se divide, cada servidor almacena un subconjunto único y no superpuesto de la información. Es decir, cada entrada de directorio se almacena en un servidor y sólo en uno. Una de las técnicas de la partición del directorio es utilizar referencias de LDAP. Las referencias LDAP permiten a los usuarios realizar consultas a servidores diferentes. Cuando la información se replica, la misma entrada de directorio se almacena en más de un servidor. En un directorio distribuido, alguna información puede ser particionada, mientras que otra puede ser replicada.

Las tres dimensiones de un directorio (alcance de la información, la localización de los clientes, y distribución de servidores) son independientes una de otra. Por ejemplo, los clientes repartidos por todo el mundo pueden acceder a un directorio que contiene sólo información sobre un solo departamento, y ese directorio puede ser replicado en muchos servidores. O bien, los clientes en un solo lugar pueden acceder a un directorio que contiene información sobre todo el mundo que se almacena en un único servidor de directorio.

El alcance de la información que se almacena en un directorio se da a menudo como un requisito de aplicación. La distribución de los servidores de directorio y la manera en que se dividen o duplican los datos, a menudo se puede controlar para afectar el rendimiento y la disponibilidad del directorio.

3.2 Ventajas del uso de un directorio

Un directorio específico para una aplicación podría sólo almacenar información que necesita sólo esa aplicación particular y no ser accesible por otras aplicaciones. Debido a que un

servicio de directorio con todas las funcionalidades es difícil de construir, los directorios para aplicaciones específicas son típicamente muy limitados. Estos probablemente almacenen sólo un tipo específico de información, y no tengan capacidades de búsqueda generales, no soporten replicación ni particionamiento y probablemente no tengan un conjunto completo de herramientas de administración. Un directorio para una aplicación específica, puede ser tan simple como un conjunto de archivos de texto modificables, y podría almacenarse y accederse de manera indocumentada y propietaria.

En dicho entorno, cada aplicación crea y gestiona su propio directorio específico, en donde su administración se convierte rápidamente en una pesadilla. La misma dirección de correo electrónico almacenada por la aplicación de calendario podría también ser almacenada por una aplicación de correo electrónico y por una aplicación que notifica a los operadores de los problemas en los equipos. Mantener múltiples copias de la misma información actualizadas y sincronizados es difícil, especialmente cuando interfaces de usuario diferentes e incluso los administradores de sistemas diferentes están involucrados en ese proceso.

Lo que se necesita es un directorio común, e independiente de las aplicaciones. Si los desarrolladores de aplicaciones pueden estar seguros de la existencia de un servicio de directorio, entonces los directorios específicos para aplicaciones específicas no serían necesarios. Sin embargo, un directorio común debe abordar los problemas mencionados anteriormente. Debe estar basado en un estándar abierto que sea compatible con vendedores de muchas plataformas. Debe ser accesible a través de una API estándar. Debe ser extensible de modo que pueda mantener los tipos de datos arbitrarios que necesitan las aplicaciones, y debe proporcionar plena funcionalidad sin requerir demasiados recursos en sistemas más pequeños. Dado que más usuarios y aplicaciones tendrán acceso y dependerán del directorio común, este deberá ser robusto, seguro y escalable.

Cuando este tipo de infraestructura de directorio existe, los desarrolladores de aplicaciones pueden dedicar todo su tiempo al desarrollo de aplicaciones en sí, en lugar de dedicarlo a los directorios específicos para dichas aplicaciones. De la misma manera que dependen de la infraestructura de comunicaciones TCP/IP y de la llamada a procedimiento remoto (RPC) para liberarlos de los problemas de comunicación de bajo nivel, deberían a ser capaces de delegar determinadas funcionalidades en los servicios de directorio. LDAP es el protocolo que se utiliza para acceder a esta infraestructura común de directorio. Como HTTP[9] (Hypertext Transfer Protocol) y FTP[10] (fileTransfer Protocol), LDAP se ha convertido en una parte indispensable de la suite de protocolos de Internet.

Cuando las aplicaciones acceden a un directorio estándar que está diseñado de una manera adecuada, en lugar de utilizar directorios específicos, se eliminan costos redundantes asociados a la administración, y a su vez los riesgos de seguridad son más controlables. La ventaja es que los datos se almacenan y mantienen en un solo lugar. Varias aplicaciones pueden usar

[9] *Ver **Glosario** al final del documento*
[10] *Ver **Glosario** al final del documento*

atributos de una entrada particular para diferentes propósitos. Aparecerán nuevos usos de la información del directorio, y una sinergia se desarrollará a medida que más aplicaciones aprovechen el directorio común.

Almacenar la información en un directorio único, y compartirlo con las diferentes aplicaciones, permitirá ahorrar tiempo y dinero así como también disminuir los esfuerzos asociados a la administración de los recursos.

3.3 Historia de LDAP y los estándares

En la década de 1970, la integración de las comunicaciones y tecnologías de computación permitieron el desarrollo de nuevas tecnologías de comunicación. Muchas de ellas propietarias e incompatibles con otros sistemas. Esto dejó en evidencia la necesidad de estándares para permitir que los equipos y sistemas de diferentes proveedores pudieran interoperar entre sí. En ese sentido, dos fueron los grandes movimientos que llevaron a desarrollar tales estándares: OSI e Internet.

3.3.1 OSI e Internet

Una unidad de los estándares fue liderado por el CCITT [11] (Comite Consultatif Internacional Telephonique et Telegraphique, o el Comité Consultivo Internacional de Telefonía y Telegrafía) y la ISO [12] (International Standards Organization). El CCITT se ha convertido en la ITU-T (International Telecommunications Union - Sector de Normalización de las Telecomunicaciones). Este esfuerzo se tradujo en la OSI (Interconexión de Sistemas Abiertos) Modelo de referencia (ISO 7498), que define un modelo de siete capas para las comunicaciones de datos con transporte físico en la capa de más bajo nivel, y los protocolos de la capa de aplicación en la capa superior.

El otro movimiento de estándares, creció alrededor de la Internet y fue desarrollado a partir de la investigación patrocinada por DARPA[13] (Defense Advanced Research Projects Agency) en los Estados Unidos. La Internet Architecture Board[14] (IAB) y su filial, la Internet Engineering Task Force[15] (IETF), desarrollaron estándares para Internet en la forma de RFCs, que después de ser aprobado, aplicado y utilizado durante un período de tiempo, eventualmente se convierten en estándares (STDs). Antes de que una propuesta se convierta en un RFC, es denominado Internet Draft.

[11] *Ver **Glosario** al final del documento*
[12] *Ver **Glosario** al final del documento*
[13] *Ver **Glosario** al final del documento*
[14] *Ver **Glosario** al final del documento*
[15] *Ver **Glosario** al final del documento*

3.3.2 Estándar de servidor de Directorio X.500

Además OSI también abordó cuestiones importantes relacionadas a grandes sistemas distribuidos desarrollados de una manera ad hoc tanto para el mercado de sistemas de escritorio como para Internet. Una de esas cuestiones importantes fueron los servicios de Directorio. El CCITT creó el estándar X.500 en 1988, que se convirtió en la norma ISO 9594, "Data Communications Network Directory, Recommendations X.500-X.521" en 1990, comúnmente conocida como X.500.

X.500 organiza las entradas de directorio en un espacio de nombres jerárquico capaz de almacenar grandes volúmenes de información. También define capacidades de búsqueda de gran alcance para hacer más fácil la recuperación de información. Debido a su funcionalidad y escalabilidad, X.500 se utiliza a menudo junto con módulos adicionales para la interoperación entre los servicios de directorio incompatibles.

X.500 especifica que la comunicación entre el cliente y el servidor de directorio utiliza el protocolo de acceso a directorio (DAP). Sin embargo dado que DAP es un protocolo de la capa de aplicación, requiere de toda la pila de protocolos OSI para operar. Soportar la pila de protocolos OSI requiere más recursos que aquellos disponibles en algunos entornos pequeños. Por lo tanto, se requería una interfaz con el servidor de directorio X.500 utilizando un protocolo que requiera menos recursos.

Acceso Ligthweight (ligero, liviano) a X.500

LDAP fue desarrollado como una alternativa a DAP más liviana. LDAP requiere la pila de protocolos TCP/IP que es más liviana y popular que la pila de protocolos OSI. LDAP también simplifica algunas operaciones X.500 y omite algunas características esotéricas.

Dos precursores de LDAP aparecen como RFCs emitidas por el IETF, Servicio de Asistencia de Directorio (RFC 1202 [4]) y DIXIE Protocolo de Especificaciones (RFC 1249 [5]). Ambos RFCs informativos que no fueron propuestos como estándares. El Servicio de Asistencia de Directorio (DAS) define un método por el cual un cliente de directorio puede comunicarse a un proxy en un servidor con "capacidades OSI" que emite solicitudes X.500 en nombre del cliente. DIXIE es similar al DAS, pero proporciona una traducción más directa que DAP.

La primera versión de LDAP se define en X.500 Lightweight Access Protocol (RFC 1487 [6]), que fue sustituido por el Lightweight Directory Access Protocol (RFC 1777 [7]). LDAP refina aún más las ideas y los protocolos del DAS y Dixie. Es más neutral respecto a las implementaciones y reduce la complejidad de los clientes para fomentar el desarrollo de aplicaciones habilitadas para directorios. Gran parte del trabajo sobre el Dixie y LDAP se llevó a cabo en la Universidad de Michigan, que proporciona referencias de implementaciones de LDAP y mantiene páginas Web y

listas de correo relacionadas a LDAP.
El RFC 1777 define el protocolo LDAP en sí. RFC 1777, junto con:
- La representación en String de la sintaxis de atributos estándar (RFC 1778 [8])
- La Representación en String de los Nombres Distinguidos (RFC 1779 [9])
- Un formato de URL LDAP (RFC 1959 [10])
- La Representación en String de los filtros de búsqueda LDAP (RFC 1960 [11])

LDAP Versión 2 ha alcanzado el estatus de draft en el proceso de normalización de la IETF, a un paso de ser un estándar. Todas las implementaciones actuales de servicios de directorio se basan en la especificación LDAPv3.

LDAP Versión 3 se define por Lightweight Directory Access Protocol (v3) (RFC 2251 [12]). RFCs relacionadas que son, o bien nuevas o bien actualizaciones para la versión 3 de LDAP son las siguientes:

- Lightweight Directory Access Protocol (v3): Definición de la sintaxis de atributos (RFC 2252 [13]).
- Lightweight Directory Access Protocol (v3): Representación de los Nombres Distinguidos en formato String UTF-8 (RFC 2253 [14]).
- La representación en String de filtros de búsqueda LDAP (RFC 2254 [15]).
- El formato de URL LDAP (RFC 2255 [16]).
- Un resumen del esquema de usuario X.500 (96) para su uso con LDAPv3 (RFC 2256 [17]).
- Métodos de autenticación para LDAP (RFC 2829 [18]).
- LDAPv3: Extensión para Seguridad en la capa de Transporte (RFC 2830 [19])
- Lightweight Directory Access Protocol (v3): Especificaciones técnicas (RFC 3377 [20]).

RFC 2251 es una propuesta de estándar, un paso por debajo de un draft. LDAP V3 extiende a LDAP V2 en los siguientes aspectos:

- Referencias: Un servidor que no almacena los datos solicitados puede referenciar al cliente hacia otro servidor.
- Seguridad: Autenticación extensible usando mecanismos autenticación simple y capa de seguridad (SASL [21]).
- Internacionalización: Soporte UTF-8 para caracteres internacionales.
- Extensibilidad: Nuevos tipos de objetos y operaciones pueden ser definidas dinámicamente y publicados a través del esquema de manera estándar.

Es decir que a partir de estas descripciones, el término LDAP se refiere LDAP Versión 3, a menos que se especifique lo contrario.

3.4 Estructura

En un servidor de directorios LDAP, la información se almacena jerárquicamente, de similar manera a como se estructura un sistema de archivos (en Unix/Linux), donde hay un nodo raíz (/), subdirectorios (/tmp, /var...), y nodos hoja (que son los archivos). A su vez, también se podría comparar con la manera en que se organizan los dispositivos en el protocolo de resolución de nombres DNS.

De igual manera que todo dentro de un sistema de archivos tiene una ubicación o "path" (por ejemplo un directorio: "/var/www/", un archivo: "/home/usuario/MiTesis.tar.bz2"), dentro de un directorio LDAP TODO tiene un **DN**, o **Distinguished Name** ("Nombre Distinguido"), el cual se indica con "dn:" y se lee desde su entrada individual, recursivamente a través del árbol, hasta el nivel más alto. Por ejemplo:

dn: o=midominio.com
....
dn: uid=tester,ou=People,o= midominio.com
....

3.4.1 La estructura de un árbol de directorio LDAP

Raíz

La raíz o nivel superior de la estructura jerárquica de un directorio se conoce como "*DN Base*", y puede ser especificada de varios modos, dependiendo de nuestras necesidades. Tomamos a modo de ejemplo el nombre de una empresa ficticia llamada *MiEmpresa S.A* radicada en *Argentina* que cuenta con un sitio web en la dirección url *miempresa.com.ar*. Las posibles representaciones del DN base son:

- **o="Nombre Organización",c="Country"**

  Esta es la forma de especificar el DN base con el formato X.500. Empleando el ejemplo de la empresa MiEmpresa el DN base con este formato podría ser**: *o="MiEmpresa S.A",c=AR*** que indica que mi empresa se llama "MiEmpresa S.A." y que el país es Argentina. Este formato ha evolucionado con el tiempo, teniendo en cuenta por ejemplo, aspectos tales como la necesidad de tener presencia en Internet.

- **o=**"URL": Esta forma de representar el DN está más enfocada a la presencia de la empresa en internet. Siguiendo con el ejemplo citado con anterioridad, podríamos representar en DN base con este formato para *MiEmpresa* de la forma ***o=miempresa.com.ar***.
- **dc=**"URL",**dc**="URL": Es como la anterior, pero desglosada. Es más similar a la manera de organizar la información como en el protocolo DNS, desglosada por componentes de

dominio. En teoría, esto puede ser levemente más versátil, aunque un poco más duro de recordar para los usuarios finales. Volviendo nuevamente al ejemplo de la empresa *MiEmpresa*, la representación de la misma empleando este formato sería ***dc=miempresa, dc=com, dc=ar***.

"Subdirectorios"

Una vez definido el DN base, empezamos a "ramificar". La manera de organizar los datos del árbol de directorio, es similar a la forma en que pensamos la organización de archivos dentro de un sistema de archivos. Es decir, que debajo de la raíz (DN base del directorio) se crean los "subdirectorios" ó contenedores para separar lógicamente los datos. Por razones históricas (X.500), la mayoría de los directorios configuran estas separaciones lógicas como entradas OU. OU viene de "Unidades Organizacionales" (Organizational Units, en inglés [22]), que en X.500 eran utilizadas para indicar la organización funcional dentro de la empresa: compras, ventas, finanzas, etc. Actualmente las implementaciones de LDAP han mantenido la convención del nombre ou, pero separa las cosas por categorías amplias como ou=gente (ou=people), ou=grupos (ou=groups), ou=dispositivos (ou=devices).

Los niveles inferiores a las OUs son utilizados a veces para categorizar hacia abajo. Por ejemplo, un árbol de directorio LDAP (sin incluir entradas individuales) podría parecerse a esto:

```
dc=miempresa, dc=com, dc=ar
    ou=customers
        ou=buenosaires
        ou=cordoba
        ou=corrientes
    ou=empleados
    ou=rooms
    ou=grupos
    ou=dispositivos
```

Registros individuales (Nodos Hoja)

Finalmente tenemos los nodos hojas, o registros individuales del árbol de directorio en donde estará contenida la información. Recordemos que cada entrada almacenada en un directorio LDAP cuenta con un único "Distinguished Name," o DN. El DN para cada entrada está compuesto de dos partes:

- El Nombre Relativo Distinguido (RDN por sus siglas en inglés, Relative Distinguished Name)
- La localización dentro del directorio LDAP donde el registro reside.

El RDN es la porción del DN que no está relacionada con la estructura del árbol de directorio. La mayoría de los items almacenados en un directorio LDAP tendrá un nombre, y el nombre es almacenado frecuentemente en el atributo **cn** (Common Name). Puesto que casi todo

tiene un nombre, la mayoría de los objetos en LDAP utilizarán su valor **cn** como base para su RDN. Podríamos decir entonces que el RDN es el nombre "corto" de un objeto dentro del directorio. Volviendo a la analogía realizada con los sistemas de archivos (file systems) podríamos decir:

- Path completo de un archivo(equivalente al DN): /etc/samba/smb.conf
- Nombre verdadero del archivo (equivalente al RDN): smb.conf

Un ejemplo de esto llevándolo a la estructura de un árbol de directorio y empleando nuevamente el ejemplo de la empresa *MiEmpresa* podría ser:

El DN: cn=Juan, ou=usuarios, o=miempresa.com.ar
El RDN: cn=Juan

El DN: cn=pc1, ou=dispositivos, o= miempresa.com.ar
El RDN: cn=pc1

Ahora es el momento de abordar el DN de un empleado de una empresa. Para las cuentas de usuario, típicamente hay un DN basado en el **cn** o en el **uid** (ID del usuario). Por ejemplo, el DN del empleado de MiEmpresa, Juan Perez (nombre de login: jperez) puede parecerse a uno de estos dos formatos:

uid=jperez,ou=empleados,dc=miempresa,dc=com,dc=ar
(basado en el login)
LDAP (y X.500) utilizan uid para significar "ID del usuario"

cn=Juan Perez, ou=empleados,dc=miempresa,dc=com,dc=ar
(basado en el nombre)
Aquí vemos la entrada Nombre Común (CN por sus siglas en ingles) utilizada. En el caso de un registro LDAP para una persona, pensar en el nombre común como sus nombres completos.

3.4.2 Personalización de clases

Los directorios LDAP pueden utilizarse para almacenar datos de casi cualquier tipo de objetos, mientras que el objeto pueda ser descrito en términos de varios atributos. A continuación se listan a modo de ejemplo, objetos con los atributos asociados que podrían ser almacenados dentro de un directorio LDAP:

Objeto ***Empleado***. Atributos:

- Nombre completo del empleado
- Nombre de login
- Contraseña
- Número de empleado

- Correo electrónico

Objeto ***Registro de Inventario***. Atributos.

- Nombre del equipo
- Dirección IP
- Número de inventario
- Marca y modelo
- Localización física

Objeto ***Listas de contacto de clientes***. Atributos

- Nombre de la empresa del cliente
- Primer teléfono de contacto
- Fax
- Correo electrónico

Objeto ***Información de un aula ó sala de reuniones***. Atributos:

- Nombre
- Localización
- Capacidad en asientos
- Número de teléfono
- ¿Acceso para silla de ruedas?
- ¿Proyector?

Objeto ***Información de recetas***. Atributos:

- Nombre del plato
- Lista de ingredientes
- Tipo de cocina
- Instrucciones de preparado.

Objeto ***Tesis de grado***. Atributos:

- Alumno
- Director
- Título
- Objetivos
- Codirector
- Asesor profesional

El directorio puede ser personalizado para almacenar cualquier tipo de texto o dato binario. Los directorios LDAP utilizan el concepto de clases de objeto para definir qué atributos son permitidos para objetos de un tipo dado. Por tal razón, en casi todas las implementaciones LDAP, es posible extender la funcionalidad básica de un directorio LDAP para adecuarlo a necesidades específicas, o bien creando nuevas clases de objetos o extendiendo las existentes.

Los directorios LDAP almacenan toda la información como una serie de pares de atributos, cada una consistente en un tipo de atributo y un valor de atributo. Esto es completamente diferente a la manera en que las bases de datos relacionales de propósito general almacenan datos, que es en forma de filas y columnas.

3.5 Ejemplo de una entrada individual LDAP

A continuación se presenta un ejemplo de un registro LDAP. Empleamos el caso del empleado Juan Perez de la empresa MiEmpresa, y el formato empleado es el de una entrada LDIF, que es el que se emplea al momento de exportar e importar entradas del directorio LDAP.

```
dn: uid=jperez, ou=empleados, dc=miempresa, dc=com, dc=ar
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: miEmpresaPerson
uid: jperez
givenname: Juan
sn: Perez
cn: Juan Perez
cn: Juancho Perez

telephonenumber: 0221-123456
o: MiEmpresa, S.A.
mailAddress: jperez@miempresa.com.ar
mailhost: mail.miempresa.com.ar
userpassword: {crypt}3x1231v76T89N
uidnumber: 1234
gidnumber: 1200
homedirectory: /home/jperez
loginshell: /usr/local/bin/bash
```

Algunos comentarios para destacar del ejemplo antes citado. Para empezar, los valores de los atributos son almacenados con las mayúsculas intactas, pero las búsquedas contra ellos no distinguen mayúsculas por defecto con excepción de ciertos atributos (como la contraseña).

Separemos esta entrada analizando cada una de sus componentes.

dn: uid=jperez, ou=empleados, dc=miempresa, dc=com, dc=ar

Este es el DN (Nombre Distinguido) completo de la entrada LDAP de la persona que se está empleado como ejemplo, e incluyendo el “path” completo a la entrada en el árbol del directorio. LDAP (y X.500) utilizan uid para representar "ID de Usuario".

```
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: miempresaPerson
```

Uno puede asignar tantas clases de objeto como requiera a cualquier tipo de objeto dado. En el ejemplo, la clase de objeto ***person*** requiere que los campos ***cn*** (nombre común) y ***sn*** (apellido, por sus iniciales en inglés surname). Esta clase permite también otros campos opcionales, incluyendo nombre dado (givenname), número de teléfono (telephonenumber) entre otros.

La clase de objeto ***organizationalPerson*** añade más opciones a los valores de las clases ***person*** e ***inetOrgPerson*** incluyendo por ejemplo la información de correo electrónico.

Finalmente ***miEmpresaPerson*** es una clase de objeto personalizada de la empresa particular que se está analizando, a través de la cual se añadirán todos los atributos del cliente que se deseen manejar para la empresa MiEmpresa.

Como se mencionara con anterioridad, el campo ***uid*** representa la identificación de usuario (login) de la persona. Obsérvese que hay más de una entrada para el CN. Esto se debe a que LDAP permite que algunos atributos tengan múltiples valores.

Por último se puede observar la información relacionada al número telefónico, dirección de correo electrónico, el nombre del servidor de correo electrónico a emplear y otros valores relacionados como ser el directorio home de la persona, y la contraseña la cual se almacena de manera cifrada.

Podemos ver un ejemplo de la estructura jerárquica de un directorio LDAP a través de la figura 1 que a continuación se ilustra.

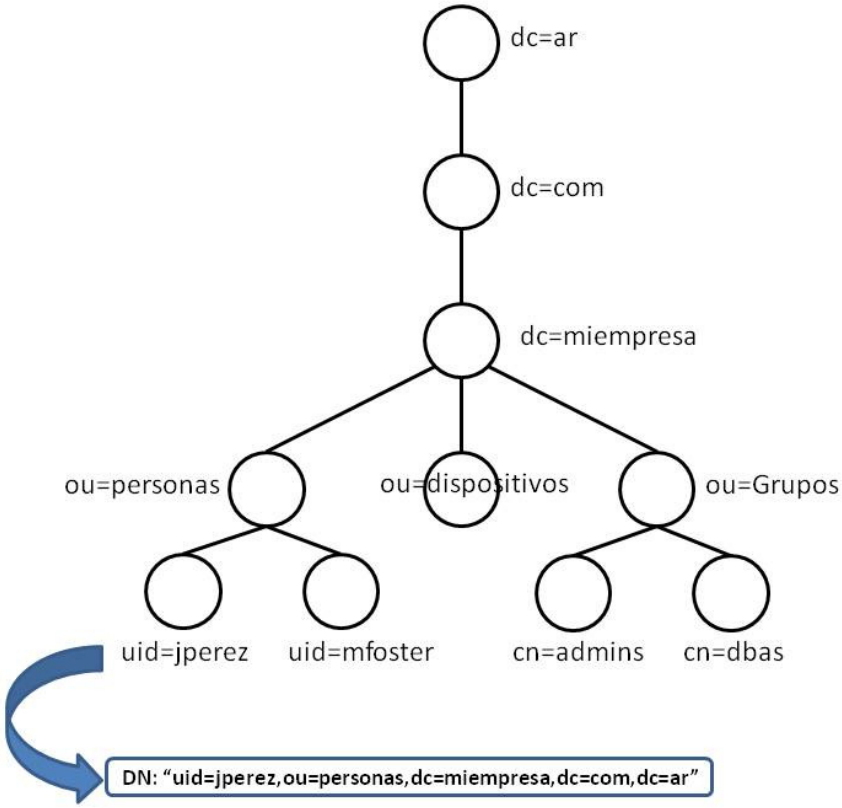


Figura 1: Ejemplo de directorio LDAP

4. Descripción del entorno

4.1 ¿Qué es y qué hace Senasa?

Para comenzar con el desarrollo del presente trabajo, me parece oportuno hacer una introducción sobre el organismo tomado como referencia: Senasa, de manera de contar con algo más de información respecto del tipo de tareas que se realizan en el mismo, para poder dimensionar la importancia del mismo a nivel Nacional. Senasa es el acrónimo de "Servicio Nacional de Sanidad y Calidad Agroalimentaria". Es un organismo sanitario cuyo principal objetivo es la fiscalización y certificación de los productos y subproductos de origen animal y vegetal, sus insumos y residuos agroquímicos, así como la prevención, erradicación y control de enfermedades animales, incluyendo las transmisibles al hombre, y de las plagas vegetales que afectan a la producción agropecuaria del país.

Para implementar y promover la acción sanitaria y fitosanitaria, elabora normas y controla su cumplimiento, asegurando la aplicación del Código Alimentario Argentino, dentro de las normas internacionales exigidas.

Asimismo, planifica, organiza y ejecuta programas y planes específicos que reglamentan la producción, orientándola hacia la obtención de alimentos inocuos para el consumo humano y animal.

El Senasa depende del Ministerio de Agricultura Ganadería y Pesca de la República Argentina [23] que depende a su vez de la Presidencia de la Nación.

Y así es que en Senasa trabajan alrededor de 6500 (seis mil quinientas) personas distribuidas por todo el país. Su infraestructura edilicia comprende:

- Una Sede Central ubicada en la Ciudad Autónoma de Buenos Aires (CABA), la cual a su vez está compuesta por cuatro edificios. Desde aquí se brindan la mayoría de los servicios críticos de la organización. De aquí en adelante a dicha red la llamaremos "*Senasa Central*".
- 14 (catorce) Centros Regionales (se trata de las oficinas más importantes ubicadas en el interior del país. A través de la figura 2 se puede observar la distribución de los Centros Regionales en el mapa de la República Argentina.
- 12 Oficinas denominadas "principales" por su tamaño, cantidad de operaciones allí realizadas, y cantidad de gente que allí trabaja. Dependen funcionalmente de los centros regionales.
- Casi 400 (cuatrocientas) Oficinas Locales que dependen de los Centros Regionales
- 2 (Dos) Laboratorios
- 1 (Una) Estación de Cuarentena
- Más de 100 (Cien) pasos de frontera entre puertos, aeropuertos y otros.

Y en todos los casos, de alguna u otra manera cada uno de estos puntos se encuentra conectado a los demás a través de una gran red, que es la que motiva la realización del presente trabajo.

Dichas dependencias se encuentran a lo largo y ancho de la República Argentina, desde Tierra del Fuego hasta Jujuy, sin dejar de tener presencia en ninguna provincia argentina. Desde las mismas son "consumidos" muchos de los servicios e información que son ofrecidos desde *Senasa Central*. Pero cabe aclarar que cada una de estas dependencias es a su vez, generadora de información la cual debe, algunos casos, ser reportada a *Senasa Central*, o bien a otra dependencia.

Figura 2: Centros Regionales en Argentina

4.2 Situación Inicial

La cantidad de dependencias implicadas en el análisis, supone una gran heterogeneidad de tecnologías, tanto la que podemos encontrar en los vínculos de red, como la del equipamiento disponible en las oficinas. En muchos casos, como por ejemplo para el caso de los enlaces de red, las tecnologías dependen de la disponibilidad de cada sector del país. Pues es sabido que cuanto más cerca nos encontramos de los centros poblacionales más importantes, mayor es la oferta de insumos relacionados con la tecnología como ser:

- Vínculos a internet
- Compra de equipamiento o repuestos/ejecución de garantías
- Recursos humanos capacitados para la instalación de una UPS, tendido de red, del cableado estructurado entre otras tantas otras.

Este ha sido una de las grandes dificultades que nos toca enfrentar cada vez que se desea llevar a cabo alguna tarea significativa en algún lugar alejado de los centros poblacionales importantes, pues en la mayoría de los casos, dichas tareas deben ser realizadas por personal que

debe viajar desde *Senasa Central*, o bien desde otra oficina más cercana. Y está claro que no todas las dependencias pueden ser ubicadas en cercanía de los centros poblacionales para poder contar con los beneficios de la mayor oferta de servicios, dado que la ubicación es en muchos casos, un aspecto estratégico de vital importancia para la dependencia. Como ejemplo de ello se puede citar a dependencias ubicadas en pasos fronterizos y puertos en los cuales la ubicación juega un rol determinante.

Por esta razón la red informática del organismo está conformada por distintas tecnologías, distintas prestaciones, distintos proveedores. Aspectos que en algunos casos suelen dar un valor agregado a la complejidad del problema a resolver.

Cada una de estas dependencias, cuenta con aplicaciones y servicios locales, los cuales a su vez podrían ser ofrecidos o utilizados desde otras dependencias. Esto se debe a que en cada región del país varían significativamente los "focos" en las actividades llevadas a cabo, pues por ejemplo las infecciones o amenazas sobre la calidad agroalimentaria no suelen no ser las mismas, así como tampoco lo son los productos producidos en las distintas regiones. Por ejemplo provincias del noroeste Argentino cuyos principales intereses podrían estar dados por el cultivo de porotos y soja, la producción de vino en Cuyo, frutícola en Río Negro, de azúcar en Tucumán, el algodón en Chaco sólo para citar algunos ejemplos Es decir que cada región presenta intereses bien focalizados en determinados productos y por ende también, son afectados por diferentes problemáticas como por ejemplo, las plagas que acosan sus cultivos y las estaciones del año en las que las mismas atacan con mayor intensidad [24].

Con esto lo que se quiere destacar es que, en varios casos, recursos tales como información almacenada en bases de datos físicamente ubicadas en la dependencia *X*, podría ser utilizada por la dependencia *Y* ubicada en otra provincia del país. Esta necesidad de compartir recursos no suele ser una complicación mayor en casos en donde la red se diagramó con antelación para abarcar ese tipo de actividades. Pero en otros casos, si bien las redes sirven principalmente para compartir recursos distribuidos geográficamente, algunas tareas no son simples. Esta simplicidad no sólo tiene que ver con los enlaces de red, sino también con aspectos como que al ser estructuras totalmente independientes, no tienen ni siquiera mecanismos de autenticación en común como para poder llevar a cabo al menos una validación de credenciales entre ellas para así agregar al menos, un mínimo de seguridad en el acceso a los recursos.

Una breve descripción de la organización lógica y física de la red del Organismo, colaborará para hacer entender aún mejor al lector los problemas que se desean abordar. Empleando algunos gráficos, se intentará aclarar las falencias sobre las que se focaliza el análisis.

Dentro del alcance de la red de lo que llamamos *Senasa Central*, trabajan alrededor de 2000 (dos mil) personas. Las mismas se encuentran distribuidas en 4 (cuatro) edificios principales distantes entre sí por unos 200 (doscientos) metros máximo. Allí se nuclean la mayoría de no sólo los recursos informáticos que forman parte de la infraestructura del organismo, tales como:

- Estaciones de trabajo

- Servidores
- Aplicaciones
- Repositorios de Información

sino también de los usuarios que acceden de manera diaria a dichos recursos. La mayoría de esos recursos están agrupados de manera lógica mediante un *Servicio de Directorio*. Por ahora sólo diremos que el mismo nos ayudará a hacer uso de manera más sencilla, ordenada y eficiente de los recursos disponibles en la red y que es donde se almacenarán las credenciales de los usuarios que deseen acceder a dichos recursos.

4.2.1 Infraestructura de red del Organismo

Lo que será descripto en la presente sección tiene que ver, como su título lo dice, con la infraestructura física de la red que sustenta al Organismo. Sin duda este ítem no es un detalle menor, ya que forma parte de la columna vertebral de las comunicaciones de cualquier organización y repercute en la mayoría de los flujos de información de los mismos. Sin lugar a dudas, "la red" es la piedra fundamental a tener en cuenta a la hora de planificar modificaciones estructurales como las analizadas en el presente trabajo. Y como veremos luego, la gran parte de las decisiones tomadas tendieron a no proponer modificaciones en lo que tiene que ver a este aspecto sobre la infraestructura ya existente. Razón de ello es que cualquier tipo de cambio menor sobre la misma, podría afectar en mucho ciertos plazos de tiempo que se desean respetar.

Desde el punto de vista físico, podemos decir que el Organismo cuenta con un mapa de red en estado avanzado, y que a través del mismo cualquier dependencia de Senasa ubicada en cualquier punto geográfico de la Argentina, debería tener conectividad con cualquier otra dependencia. Con esto quiero destacar que la infraestructura existente al momento, colaboró en mucho en las decisiones tomadas a la hora de buscar la mejor solución para varios de los problemas presentados.

Como se comentara con anterioridad, Senasa está compuesto por gran cantidad de dependencias las cuales a su vez cuentan con distintos roles dentro las actividades llevadas a cabo por el Organismo, y como es de esperar se cuenta con dependencias de gran tamaño (en volumen de información generada, cantidad de usuarios, cantidad de PCs, etc) y otras de menor envergadura. Por esta razón podemos hacer una disgregación de las dependencias de acuerdo a la cantidad de personas que trabajan en las mismas y ordenarlas según una estimación de su volumen de información y usuarios como se detalla a continuación:

- Senasa Central
- Centros Regionales
- Oficinas denominadas Principales

- Laboratorios
- Estación de cuarentena
- Oficinas Locales
- Puertos, aeropuertos y otros pasos de frontera

A partir de esta clasificación, diremos que tanto los Centros Regionales, como las oficinas principales, como los Laboratorios como la Estación de Cuarentena cuentan con "privilegios" con respecto al resto a la hora de hablar de la conectividad. Esto es porque cada una de estas dependencias cuenta con un enlace de tipo "dedicado" (red MPLS[16]) de al menos 1 Mbps[17] de ancho de banda que las vinculan con *Senasa Central*. Es decir que dichas dependencias están "directamente conectadas" a través de un vínculo provisto por algún ISP (Internet Service Provider)[18] a *Senasa Central*. De más está decir que estas dependencias son las que cuentan con las mejores aptitudes desde el punto de vista de la conectividad, y por ende cuentan con condiciones para poder llevar a cabo la compartición de recursos e información de la manera más prolija de acuerdo a lo analizado en este documento. De aquí en adelante, llamaremos a las dependencias con enlace dedicado como el aquí descripto Dependencias "Tipo 1". Estos vínculos dedicados brindan a las dependencias un enlace por demás aceptable para mantener una interacción fluida desde el punto de vista operacional con la oficina principal denominada *Senasa Central*.

Además del mencionado enlace dedicado, estas dependencias cuentan (en la mayoría de los casos) con un segundo vínculo pero de menor ancho de banda generalmente del tipo ADSL[19], a través del cual se vinculan con Internet. Es decir, que todo el tráfico que sea hacia la red corporativa se envía a través del enlace dedicado que las une con casa central, y todo el tráfico que tenga como destino el "resto del mundo" es encaminado a través del vínculo ADSL.

Para poder tener una visión más clara de lo que aquí se describe, a continuación se presenta una figura que lo ilustra de manera simple (Figura 3):

[16] *Ver **Glosario** al final del documento*
[17] *Ver **Glosario** al final del documento*
[18] *Ver **Glosario** al final del documento*
[19] *Ver **Glosario** al final del documento*

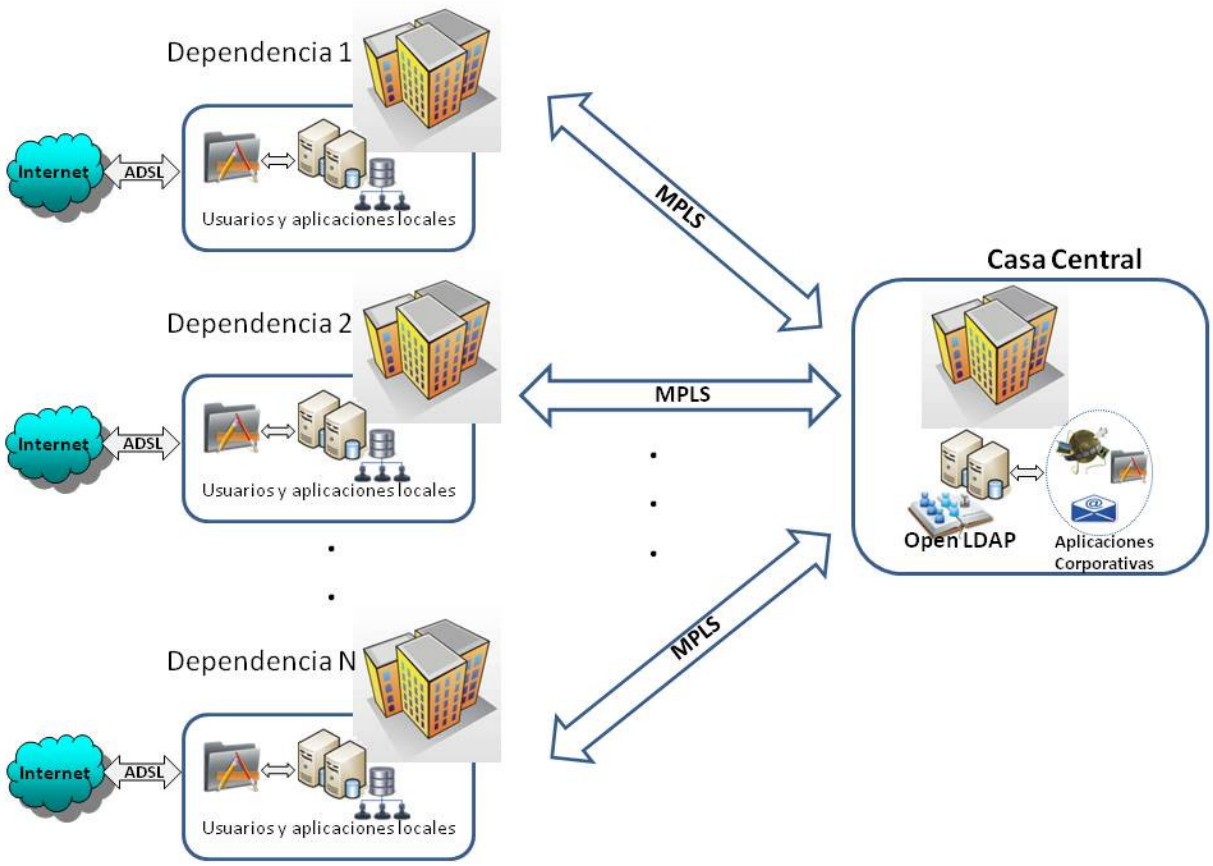


Figura 3: *Situación Actual para Centros Regionales, Oficinas principales, Laboratorios, y Estación de Cuarentena (Dependencias Tipo 1)*

Pero la situación es muy diferente para las dependencias más pequeñas como Oficinas locales y Puertos, aeropuertos y otros pasos de frontera, pues en estos casos no se cuenta con un enlace dedicado que las vincule con *Senasa Central*, sino que sólo se cuenta con un enlace en su mayoría de tipo ADSL a través del cual se conectan a Internet. Es decir, que para este tipo de dependencias, toda conexión con *Senasa Central* y otras dependencias se realiza a través de un enlace compartido, inseguro y por momentos inestable. De hecho, el 100% de su conectividad con el resto del organismo depende del estado de dicho enlace. O sea, que en caso de no funcionar el mismo, su conectividad con el resto del organismo se verá interrumpida. De aquí en adelante llamaremos a este tipo de dependencias como Dependencias "Tipo 2" y se ilustran mediante la Figura 4.

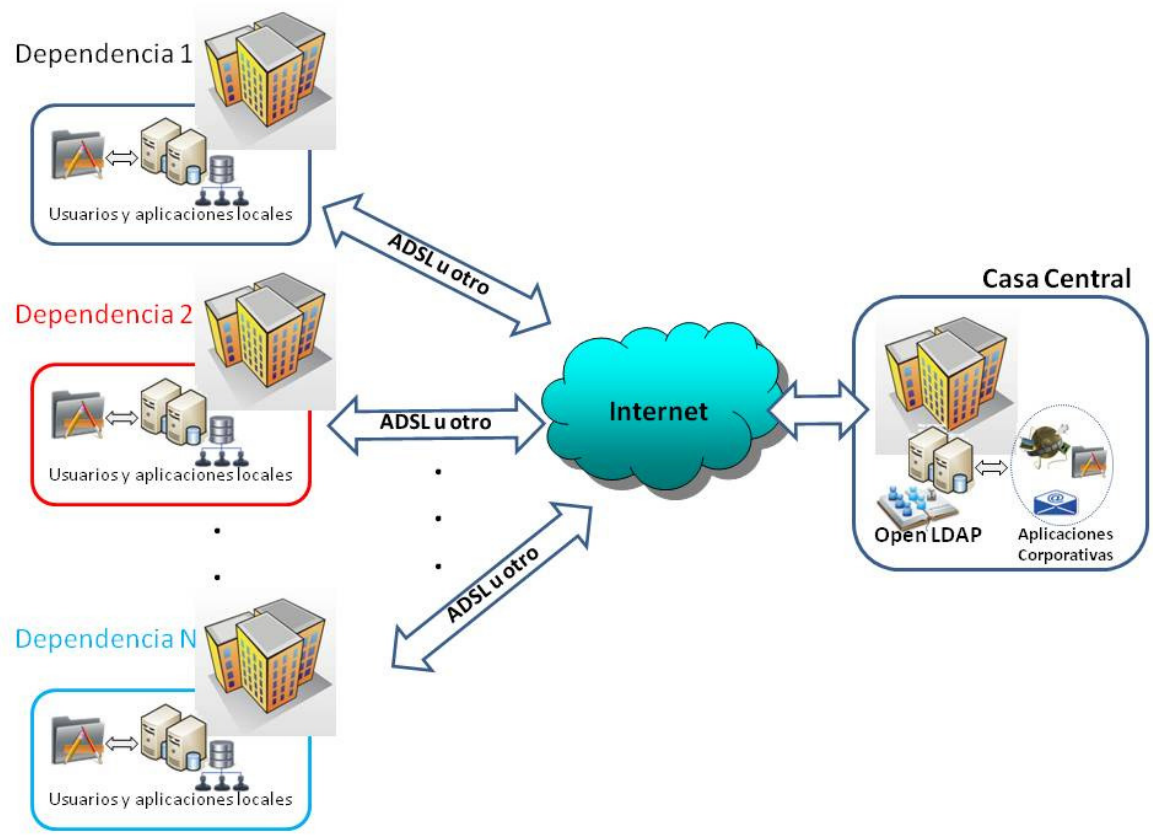


Figura 4: Situación Actual para Oficinas locales, Puertos, aeropuertos y otros pasos de frontera (Dependencias Tipo 2)

Podemos observar a través de la figura 3, que las dependencias de Tipo 1 cuentan con dos enlaces distintos: uno dedicado y directamente dirigido a casa central (MPLS), y otro a Internet (ADSL). Mientras que para los casos descriptos a través de la Figura 4 (dependencias Tipo 2), sólo se cuenta con un único enlace (ADSL), mediante el cual las dependencias se vinculan con el resto de la red. En este segundo caso, la conectividad dependerá en su totalidad del estado de ese único vínculo, mientras que en las dependencias del primer caso, se podrán llevar a cabo tareas de contingencia de algún tipo en caso que alguno de los dos enlaces se vea interrumpido, de manera de no sufrir discontinuidad en los servicios, o bien para que la misma sea mínima.

4.2.2 Infraestructura de Servicios

Esta sección introduce al lector a los servicios que se prestan desde cada uno de los distintos tipos de dependencias con las que cuenta el Organismo. Esto, sumado a la infraestructura de red que fue descripta en la sección anterior, nos permitirá tener una visión más clara de la manera en que el consumo de red y servicios se lleva a cabo, y así poder identificar más fácilmente las falencias con que nos encontraremos.

Conocer detalles de las dependencias tales como cantidad de equipos, cantidad de usuarios, servicios ofrecidos, servicios consumidos, entre otros, nos permitirá entender mejor algunos aspectos analizados en el presente trabajo.

La descripción de la infraestructura de servicios del Organismo, la dividiremos de acuerdo a los servicios presentes en cada tipo de dependencia de manera de hacerlo más claro. Es decir, será dividido en *Senasa Central*, dependencias de Tipo 1 y dependencias de tipo 2.

Senasa Central

Iniciamos la descripción con *Senasa Central*, que como ya se dijera en párrafos anteriores podríamos decir que se trata de la dependencia más importante del Organismo desde el punto de vista administrativo, operativo, en cuanto a cantidad de gente que allí opera, infraestructura, servicios prestados, servicios consumidos, etc. Es desde aquí que se brindan casi la totalidad de los servicios que llamamos corporativos, es decir, aquellos que son consumidos desde todo el resto del país.

- Está conformada por aproximadamente 1300 (un mil trescientos) equipos sólo teniendo en cuenta las estaciones de trabajo de usuario. Las mismas poseen instalado alguna de las versiones disponibles de la familia de sistemas operativos de Microsoft, como son Windows XP, Windows Vista, Windows 7.

- Con respecto a lo que es servidores, se cuenta con más de 150 (ciento cincuenta) equipos entre los cuales podemos encontrar más heterogeneidad en cuanto a sistemas operativos, alguno de ellos son de la familia de sistemas operativos de Windows, mientras que otros son distintas distribuciones de Linux[20].

- La cantidad de PCs de usuario de esta red, está en etapa de continuo crecimiento.

- En esta red se encuentra funcionando un Servicio de Directorio a través de la herramienta provista por la herramienta propietaria de Microsoft denominada Active Directory[21]. A dicho servicio de directorio lo denominaremos de aquí en adelante ***ADS senasa*** (como acrónimo de Active Directory Service), de manera de poder referenciarlo más fácilmente. Esta herramienta es ideal en grandes entornos corporativos en donde se requiere contar con un inicio de sesión en las terminales de usuario controlado. Es decir, en donde se pueda definir en un único lugar y de manera centralizada, quiénes y con qué roles podrán hacer uso de los equipos que forman parte de la red.

[20] *Ver **Glosario** al final del documento*
[21] *Ver **Anexo I**: "Active Directory Service (ADS)" para más información*

- ***ADS senasa*** nucleaba menos del 20% de las terminales de usuario al momento de iniciado el presente trabajo, y se encontraba soportado por dos servidores cuyo rol dentro del servicio, es el de controladores de dominio. A través de este servicio, los usuarios pueden iniciar una sesión interactiva en cualquiera de los equipos que forman parte del mismo, ingresando credenciales (usuario/clave) almacenados en las bases de datos de ***ADS senasa***. Cabe destacar que este repositorio SÓLO efectúa la validación de usuarios de *Senasa Central*.

- Los recursos pertenecientes a ***ADS senasa*** (usuarios, equipos, políticas de seguridad, repositorios de archivos, etc) son de uso exclusivo de aquellos usuarios o equipos que forman parte de dicho servicio de directorio. Aunque cabe mencionar, que si bien aquellos usuarios o PCs que no forman parte del servicio de directorio pueden hacer uso de los recursos allí contenidos, este "uso" no es transparente, y en la mayoría de los casos se realiza bajo medidas de seguridad pobres y de complicada administración y mantenimiento.

- En la red de *Senasa Central*, existe a su vez un segundo servicio de directorio implementado a través de herramientas libres para uso de LDAP, el cual sirve a diversas aplicaciones utilizadas. Es decir, que un gran número de aplicaciones y sistemas que se encuentran en producción, no se validan contra ***ADS senasa***, sino contra este segundo repositorio de credenciales de usuario basado en LDAP, el cual denominaremos de aquí en adelante ***LDAP senasa***. Esto significa que se cuenta con dos repositorios de usuarios diferentes para almacenar las credenciales para el acceso a distintos recursos. Y recordemos que por el momento, sólo estamos hablando de la red de casa central. Para entender mejor la diferencia de estos dos servicios de directorio una figura facilitará el asunto. Para ello la figura 5 nos permite visualizar que el servicio de directorio ***ADS senasa*** (implementado a través de Active Directory) tendrá alcance sólo para aquellas PCs y usuarios que se encuentren incorporados a dicho servicio de directorio. En esos casos, nos permitirá acceder a los recursos tales como carpetas compartidas, inicio de sesión en las PCs así como también nos facilitará la integración con gran cantidad de otros servicios sobre los cuales no entraremos en detalle aún. Por otro lado, el restante servicio de directorio implementado con herramientas abiertas de LDAP (***LDAP-senasa***), es el encargado de llevar a cabo la validación para acceder a la gran mayoría de las aplicaciones implementadas dentro del organismo así como también servicios tales como el correo electrónico, y la navegación por internet por proxy[22] web, servicios que cabe destacar son consumidos desde todo el país, y no sólo desde *Senasa Central*. La figura 6 ilustra lo descripto.

[22] *Ver **Glosario** al final del documento*

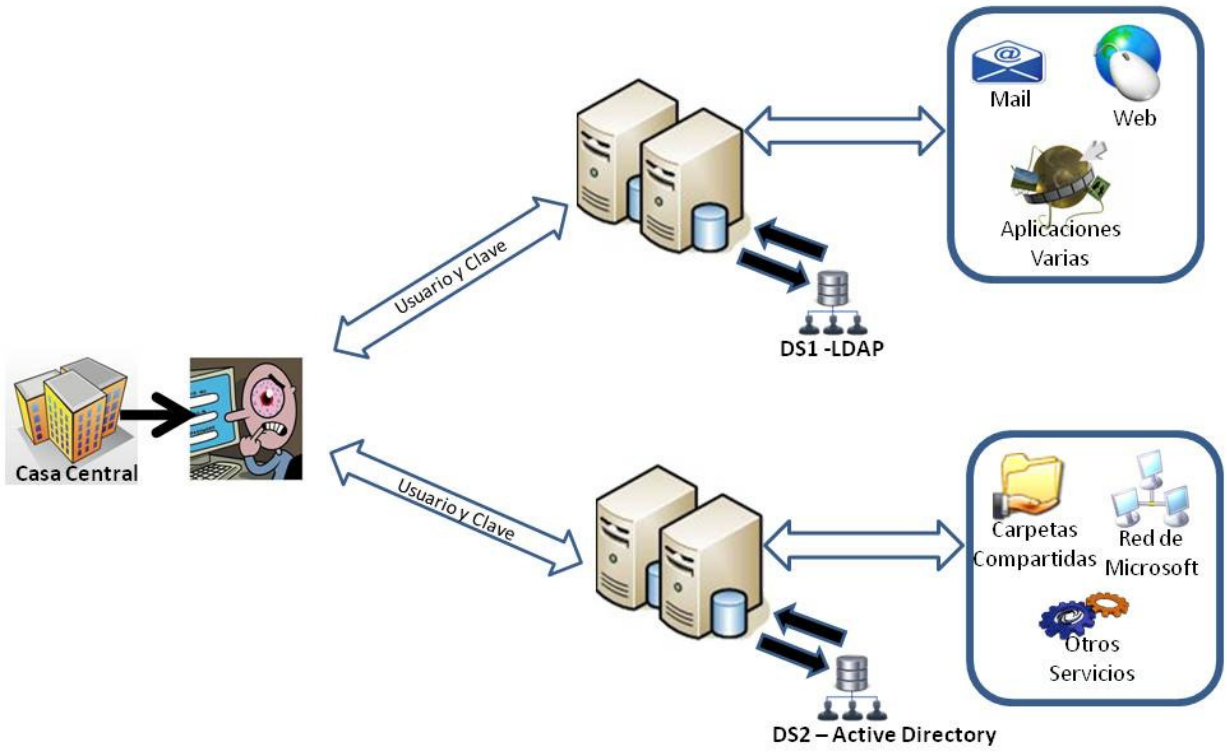


Figura 5: En Central, dos Servicios de Directorio me permiten acceder a distintos recursos de la red

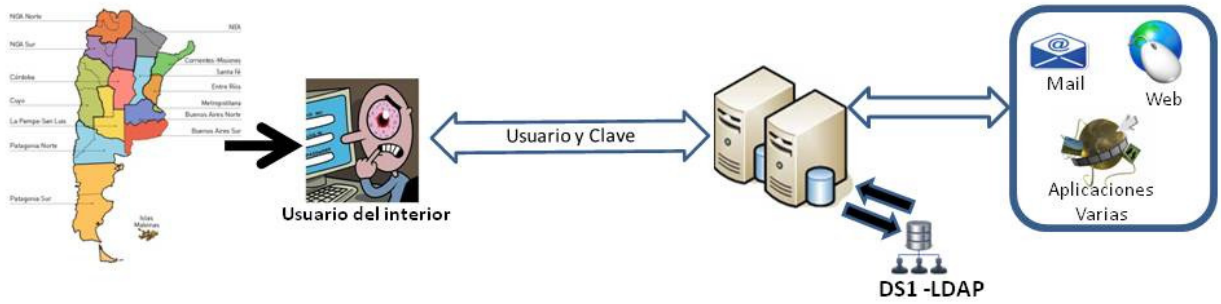


Figura 6: Servicio de directorio de LDAP con alcance para todo el país

Dependencias (de Tipo 1)

A continuación se brindará una descripción de las dependencias que denominados de tipo 1 y por qué este tipo de dependencias fueron tratadas de una forma distinta respecto al resto. Recordemos que nos estamos refiriendo a los Centros Regionales, Laboratorios, Estación de Cuarentena y la razón es que dichas dependencias comparten entre sí algunas características en

cuanto a su infraestructura y a su vez se tratan de las más importantes en cuanto a cantidad de personas que agrupan, equipamiento involucrado, servicios brindados, y relevancia operacional.

Esta información es de vital importancia para la toma de decisiones a la que apunta el presente trabajo, y nos permitirá contar con un panorama más amplio en cuanto a lo referente al esquema organizacional de Senasa.

A su vez, se describen los servicios que se podrían llegar a prestar desde las mismas. Cabe recordar que dichas dependencias se encuentran dispersas a lo largo y ancho de nuestro país.

- En cuanto a la cantidad de equipos de usuario, tenemos dependencias que contienen unas pocas PCs (menos de 20) y otras de mayor tamaño con más de 160.

- En lo que respecta al tipo de enlace que lo vincula con *Senasa Central*, en todos los casos que englobamos aquí se cuenta con vínculos dedicados tipo MPLS de no menos de 1 Mbps (megabit por segundo) de ancho de banda. Esto nos garantiza una conectividad con una estabilidad aceptable, indispensable para diagramar esquemas de replicación e intercambio de información constante como se verá más adelante.

- En algunas dependencias, las redes locales de las mismas agrupan los recursos a través de un servicio de directorio empleando la herramienta de Microsoft Active Directory de similares características al implementado en casa central (que denominamos ***ADS senasa***), pero en todos los casos, se trata de estructuras completamente independientes entre sí y sin compartición alguna de datos y/ó información con esta última.

- La mayoría de las dependencias no cuenta con personal técnico capacitado para realizar las tareas complejas de administración y/ó configuración de los equipos de red ó servidores locales, o bien el personal disponible es insuficiente para la cantidad de requerimientos relacionadas a tecnologías de la información dado que cuentan con otras tareas no relacionadas con el ámbito de la tecnología. Esto significa que en caso de ser necesario llevar a cabo alguna tarea sobre los equipos de dicha red que no pudiera ser realizados a través de las herramientas de administración remota, personal perteneciente a *Senasa Central* debería hacerse presente en las instalaciones de la dependencia con todo lo que ello implica en cuanto costos en lo que tiene que ver a lo económico, como en el mayor tiempo para que la solución se vea implementada. Tiempos que en muchos casos se convierten en prohibitivos, sin mencionar que el recurso humano involucrado en tareas relacionadas a tecnología de la información suele ser insuficiente. Este punto aunque por momentos resulte difícil de creer, se ha convertido en uno de los escollos más importantes a superar, pues tanto las tareas a realizar, como la lejanía de los lugares a donde las mismas debían ser efectuadas, sumado a la escasez de recursos humanos, se convierten en el factor desencadenante del atraso de muchas de las tareas fundamentales para el avance del presente proyecto.

- En la mayoría de los casos se necesita compartir recursos de manera local (archivos, impresoras, información contenida en bases de datos nuevas o históricas de una región) entre las personas pertenecientes a la misma dependencia, o bien entre personas pertenecientes a distintas dependencias de manera de evitar contar con duplicidad de información.

- Todas las dependencias emplean como sistema operativo de escritorio, productos de la empresa Microsoft (Windows) [25]. Esta homogeneidad es un aspecto de gran relevancia a la hora de definir las herramientas a emplear entre otros.

- Muchas dependencias cuentan con sistemas propios, bases de datos propias, servicios propios que pueden o no ser compartidos por otras dependencias o por usuarios ubicados en *Senasa Central*. Estos se autentican contra repositorios de usuario locales, que nada tienen que ver con alguno de los hasta aquí mencionados.

- Cada dependencia cuenta con su repositorio local de usuarios, y a su vez los mismos no son compartidos en ningún caso. Esto significa que no es posible emplear los usuarios de una red para hacer uso de los recursos de otras redes. Si eso fuera requerido, los usuarios deberían ser definidos de manera repetida en los repositorios de cada una de las dependencias en los que necesite acceder.

- Como ya se ha mencionado, algunos servicios provistos por *Senasa Central*, son usados por todo el Organismo. Ejemplo de ello es el servicio de correo electrónico que se implementa en forma centralizada. Esto implica que todos los usuarios que cuentan con una cuenta de correo, deben estar definidos de alguna manera en algún repositorio de cuentas de usuarios en forma centralizada y de hecho lo están en ***LDAP senasa*** del cual ya se hizo mención. Dichos usuarios, no tienen por qué coincidir con los que se definen para hacer uso de los recursos de la red local de la dependencia. Por tal razón, podría darse el caso y de hecho sucede que una persona cuente con muchos usuarios distintos, con identificadores distintos, y obviamente, claves distintas. Como para dar un ejemplo, podríamos tener el caso de Juan Pérez cuyo nombre de usuario para uso del correo electrónico podría ser *jperez*, y el definido para acceder a la base de datos de la dependencia a la que pertenece podría llegar a ser *juanp*. A su vez también podría darse el caso que nombres de usuario iguales definidos en distintos repositorios de información, pertenezcan a distintas personas. Por ejemplo, que el nombre usuario *jperez* definido en la base de datos X, pertenezca a Juan Pablo Pérez, y que el nombre de usuario *jperez* definido en la base de datos Y, pertenezca a Julieta Pérez.

De lo descripto hasta aquí resaltaremos algunos aspectos puntuales a fin de destacar algunos detalles de la situación analizada y de las propuestas de cambio:

- No existen políticas ó directivas centralizadas que apunten a definir las buenas prácticas y la seguridad sobre el uso de los recursos relacionados con la información. Esto dificulta en gran medida tareas tales como la manera en la que los usuarios son definidos en cada una de las dependencias, la manera en la que la información es almacenada y resguardada, la definición del uso aceptable de internet, así como tantos otros aspectos relacionados con la seguridad de la red y de los recursos informáticos, pues en muchos casos ciertas decisiones son tomadas de manera disjunta por el responsable de cada dependencia teniendo una diversidad de criterios en muchos casos inaceptable. Cualquier tipo de política de este tipo que se desee aplicar, deberá ser definida y aplicada de manera independiente en cada uno de los ámbitos.

- Imposibilidad de aplicar procedimientos y seguimiento de aspectos relacionados con la auditoría de eventos. La causa radica en la imposibilidad de interrelacionar eventos entre equipos con distintas administraciones además de la imposibilidad de identificar a una persona en base al usuario empleado para el acceso a la información, ya que en muchos casos, los usuarios no identifican unívocamente a las personas. A eso podemos sumar la inexistencia de directivas que indiquen el tiempo que deba ser almacenado un registro de log.

- Imposibilidad de aplicar configuraciones generalizadas para toda la red corporativa de manera global y unívoca. Los equipos de la red deben ser configurados en forma descentralizada e individual. En caso de desear contar con configuraciones similares, las mismas deberían ser confeccionadas tantas veces como instancias se deseen, debido a que en muchos casos los equipos son de administraciones distintas.

- Resulta complicado compartir recursos entre dependencias. Esto tiene que ver con que los recursos son empleados de distinta manera de acuerdo a la dependencia, definidos de distinta manera, y también dado que no hay usuarios en común para hacer uso de los recursos de manera autenticada.

- Desde *Senasa Central* resulta imposible conocer los recursos disponibles en las dependencias si no es a través de una visita a la red correspondiente. A su vez, cualquier dispositivo que sea conectado en la red de la dependencia, podría ya sea de manera involuntaria o malintencionada, interferir en el funcionamiento de la red de manera negativa. Y esto podría lograrse de manera muy sencilla, pues los mecanismos para evitarlos son muy escasos o nulos. A su vez, esto sería muy difícil de detectar.

- En algunos casos, la administración de los recursos disponibles en las dependencias debe ser realizada sólo desde la misma dependencia. Esto se debe a que no se cuentan con mecanismos claros para ganar acceso a todos los recursos por distintos motivos (direcciones variantes, desconocimiento, falta de herramientas, etc.)

- No se emplea un repositorio unificado de usuarios para el acceso a los recursos de la red local por lo cual, el personal responsable de llevar a cabo tareas de administración debe contar con una cuenta de usuario en cada uno de los equipos que desee administrar. Esto puede resultar en una estructura difícil de mantener y configurar. Y en muchos casos, la consecuencia es el uso de usuarios genérico que son manipulados por varias personas y que por ende no identifican unívocamente a quien los emplea con todas las observaciones desde el punto de vista de la seguridad que ello amerita.

- No existe un repositorio unificado de información en donde todos los usuarios del organismo puedan almacenar sus archivos de manera centralizada. Esto dificulta tareas como la realización de copias de seguridad, definición de políticas relacionadas a la seguridad entre otras. A su vez, crea cúmulos de información duplicada pues se vuelve imposible saber si la información se encuentra ya en otro repositorio en otra dependencia, difícil de depurar, acceder dando como resultado información de menor valor. Este punto ha sido un foco de observación en varias oportunidades de auditorías tanto internas como externas al Organismo.

Esta es una lista de algunos de los problemas que se observaron y que llevaron a tomar alguna decisión de tipo estructural sobre la manera en que los recursos de información son manejados. Pero como vemos, no se hizo una introducción demasiado profunda acerca de las dependencias de tipo 2. Y esto tiene una explicación que incidirá notablemente a favor de los cambios a introducir, y que se irán analizando a lo largo de todo el documento. Esto tiene que ver con la decisión política que las dependencias de tipo 2 tiendan a convertirse todas en dependencias de tipo 1. Para ello son varios los aspectos que deberán modificarse en las mismas, pero esta determinación unificará de alguna manera el universo de dependencias y ayudará a pensar las soluciones de una manera más integral, sin tener que tomar el caso de las dependencias de tipo 1 como casos excepcionales teniendo en cuanta su cantidad, sino por el contrario asumiendo dicha estructura como la generalidad.

Esto significa que si bien al momento de realizado el análisis del presente trabajo el entorno es el descripto, cabe aclarar que la solución a adoptar asume la premisa de una infraestructura más homogénea en donde no exista la disparidad estructural previamente introducida entre las dependencias de tipo 1 y 2, o bien la misma sea menor.

Cabe destacar también, que en algunos pasajes del documento, se hace la distinción en aspectos relacionados a la implementación y se destaca que la misma tiene sentido en dependencias de tipo 1 teniendo en cuenta la premisa que se acaba de citar, en donde se intenta tomar como dicho tipo de dependencia como generalidad.

5. Desarrollo

¿Qué problemas se desean resolver? ("Conjunto de partes" VS "Partes de un todo")

Los principales problemas que se desean abordar son en esencia y a gran escala dos, los cuales se fueron introduciendo a lo largo del documento. El problema aquí no sólo es de la infraestructura del Organismo, sino que más bien se trata cada vez más de un problema creciente que las personas comunes tenemos a la hora de usar servicios de distinto tipo. A decir, servicios tales como el cajero automático, el home banking, el correo electrónico, el chat y cualquier otro que se haga llamar seguro, requiere de credenciales para autenticarnos (mínimamente usuario y contraseña). Esto significa, que para cada uno de estos servicios tendremos que recordar/guardar de manera segura todas las credenciales asociadas. Tarea por demás complicada, o casi imposible sin incurrir en una ayuda memoria (como podría ser la mala práctica de escribir las claves en un papel).

Senasa no es un caso distinto. Como se desarrollara en párrafos anteriores la demanda de servicios y aplicaciones desde el Organismo hacia las áreas de tecnología es una constante en crecimiento. La diversidad de aplicaciones, sistemas y demás medios tecnológicos para el acceso a la información, planteó la necesidad de ocuparnos del tema del manejo de credenciales de manera centralizada, teniendo en cuenta que algunas aplicaciones ya contaban con sus propias bases de datos lo cual hacía aún más complejo tareas tales como la integración entre aplicaciones, así como también obligaba a los usuarios a contar con distintas credenciales de acceso dependientes de los sistemas empleados. Todo esto sin entrar en la complejidad aún mayor que tendríamos a la hora de hablar de los roles o perfiles de acceso que cada usuario tendría en cada una de las aplicaciones/servicios con las credenciales asociadas, porque estaríamos entrando en una matriz de combinaciones casi infinita de opciones.

Pero para buscar una solución, debemos tener en claro cuál es el verdadero problema que queremos abordar. Y en el caso de este análisis se hará foco en un gran problema inicial, que a medida que se vaya planteando la solución elegida, introducirá nuevos interrogantes, y nuevos problemas propios de la misma solución. Por esta razón, la solución será planteada en dos etapas claramente identificables que se irán clarificando de aquí en adelante.

A partir de aquí se pondrá foco en los aspectos a ser analizados dentro de la infraestructura estudiada para hacer énfasis en las debilidades de la misma, y para finalmente poder contar con un abanico de alternativas posibles a implementar y así determinar la mejor de las opciones dentro del contexto en el que nos encontramos.

Una falencia que ya se mencionara a nivel infraestructura de la tecnología dentro de Senasa, tiene que ver con la **visión disgregada** de cada una de las redes que conforman el

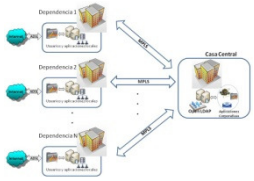
organismo. En muchos casos, y como ya se comentara a lo largo del presente documento, los recursos se agrupan y relacionan como un *"conjunto de partes"* disjuntas y casi sin nexo, y no como *"partes de un todo"*, elementos que colaboran entre sí con un fin particular de orden dentro del funcionamiento del organismo. De aquí el título de esta sección: "Conjunto de partes" que se comportan como independientes unas de otras, con una interacción pobre y compleja versus "Partes de un todo" como piezas de un mismo rompecabezas interactuando entre sí, cada una con un rol específico dentro del funcionamiento integral del Organismo, tratando en todo momento de lograr la armonía y la simplicidad. Se desea obtener un todo como infraestructura conformado por partes interrelacionadas, que dependen unas de otras. Este todo, es lo que queremos denotar como la **visión unificada de la organización**.

Para entender mejor de lo que estamos hablando, nos remitiremos nuevamente a la figura 3 en donde se ilustró que cada oficina cuenta con sus repositorio de usuarios propio y local, es decir que no hay un repositorio centralizado de usuarios a nivel Organismo y es a esto a lo que nos referimos con la visión disgregada, y la figura 5 (al menos dos grandes BDs de usuarios incluso unificando los usuarios de todas las oficinas con los de Casa Central). A partir de acá podemos ver que la problemática se divide en dos grandes casos bien definidos y a resolver:

1- Lograr obtener una visión unificada del Organismo: Donde todas las grandes oficinas se validen contra los mismos repositorios de credenciales de usuarios (planteado a través de la figura 3)
2- Unificar dichas credenciales de usuarios en una sola, de manera de no contar con múltiples definiciones de usuarios para una persona (planteado a través de la figura 5)

Ahora si tendríamos los problemas bien definidos, y podríamos empezar a abordarlos. Para ello tenemos que ver de qué distintas maneras y qué etapas tendremos que cubrir para atacarlos de la mejor manera. Es por ello que para mostrar la secuencialidad de la solución planteada, se hará un abordaje del punto 1, para luego seguir con el punto 2.

5.1 Punto 1: Visión disgregada del Organismo



Introducción

En esta sección haremos un análisis algo más detallado del problema ya planteado y descripto a través de la figura 3. Como ya se mencionara, este tipo de inconveniente surge como producto del crecimiento y expansión que el organismo ha tenido a lo largo de los últimos años tanto en su infraestructura edilicia en todo el país, como en cantidad de personal. Este crecimiento, no siempre fue acompañado de la correspondiente inversión en infraestructura

tecnológica, la cual aún al día de hoy difiere en algunos casos, de la necesaria para sustentar las innumerables necesidades informáticas del Organismo.

Los grandes problemas aquí planteados, son la gran cantidad de bases de datos de usuarios locales que existen y la relación en algunos casos nula entre ellas. A decir, al menos existe un repositorio de usuarios local en cada una de las oficinas que se analizan. No está de más volver a recordar que para este caso, nos estamos refiriendo a las oficinas del tipo 1. Y que como se mencionara con anterioridad, no se entrará en detalle con las dependencias de tipo 2, teniendo en cuenta la premisa que se prevé un futuro sólo con dependencias tipo 1.

Pero ¿qué significa que cada oficina de tipo 1 tenga su propio repositorio local de credenciales de usuario? Significa que una misma persona dentro del organismo, podría llegar a tener tantas credenciales de usuario como oficinas de tipo 1 haya para el caso en que necesitara tener acceso a los recursos locales de todas ellas. Es decir que en el peor de los casos una persona de nombre “Juan Perez” podría tener para acceder a:

- Casa Central
    - Usuario: jperez
    - Clave: clave1
- Centro Regional [23]1
    - Usuario: jperez
    - Clave: clave2
- Centro Regional 2
    - Usuario: juperez
    - Clave: clave3
- Centro Regional 3
    - Usuario: juanperez
    - Clave: clave4
- Laboratorio1
    - Usuario: juanperez
    - Clave: clave2

Además, ningún cambio realizado en alguna de las credenciales, se vería reflejado en alguna otra, dado que no existe ningún tipo de sincronismo y/ó replicación.

Sin lugar a dudas este representa un gran problema, y no sólo para el usuario que debe recordar un gran número de credenciales de acceso de acuerdo al recurso que quiera emplear, sino también para el equipo de infraestructura informática encargado de mantener un gran número de repositorios que las almacenan que a su vez son independientes entre sí.

[23] *Ver **Glosario** al final del documento*

5.1.1 Alternativas de solución

Visión unifica de la organización

Como primer desafío se presenta la tarea de unificar la visión del Organismo. Y a lo que nos referimos es justamente a proponer una integración de todas componentes que forman parte de los servicios de TI de la organización Senasa en una de mayor tamaño, logrando de esta manera una diversidad de beneficios desde el punto de vista de la administración y definición de recursos, así como también portabilidad de aplicaciones empleadas. ¿Y a qué me refiero cuando hablo de los componentes que forman parte de los servicios de TI de la Organización?

- Redes
- Información
    - Bases de datos
    - Archivos
- Definición de Usuarios (con toda la información asociada a un usuario)
    - Datos personales
    - Nombre de usuario
    - Clave
    - Roles en las distintas aplicaciones
    - Ubicación geográfica
- Procesos de validación de usuario

Como ya se mencionara con anterioridad, dentro de la versión disgregada, estos recursos son definidos de manera repetida, perdiendo en muchos casos la integridad de los mismos, y haciendo que todas las tareas asociadas a un administrador se compliquen en gran escala (además de colaborar a la pobreza de la información).

Muchos de estos beneficios tienen que ver con las características hasta aquí descriptas, las cuales dejan en evidencia una serie de falencias. Más aún teniendo en cuenta las perspectivas de crecimiento que se esperan de la red y de los dispositivos, no sólo para *Senasa Central* sino también para el resto de las dependencias existentes y las nuevas que podrían llegar a sumarse a la infraestructura.

La situación deseada sería aquella en donde toda la información se defina sólo una vez en alguna parte del organismo, y que la misma sea manejada de manera consistente por todos los actores que la necesiten. De esta manera, cualquier cambio de la información (incorporación de un nuevo usuario, modificación de cualquier dato relacionado a un usuario como ser el domicilio o bien, la eliminación de un usuario) debería ser llevado a cabo sólo en un lugar, y dicho cambio debería verse reflejado en cualquier repositorio de información que lo contenga. Estaríamos hablando de algo similar a lo que se conoce como una base de datos distribuida/replicada, en la cual la información podría encontrarse “dispersa” en distintos repositorios de datos, pero cualquier tipo de modificación a la misma debería ser llevada a cabo siguiendo condiciones que mantengan la integridad y demás aspectos deseables.

El problema que se plantea es cómo armamos esa base de datos distribuida/replicada a partir del presente de disgregación con el que nos encontramos. Y cómo hacemos para mantener de manera consistente la misma teniendo en cuenta todas las falencias que con anterioridad se describieron. Sin duda las preguntas no son de fácil respuesta, y el análisis bien vale la presente investigación.

Dentro de esta visión unificada, una de las principales metas a conseguir tiene que ver con la unificación de las bases de datos de usuarios a nivel corporativo. Tal como se mencionara, las dependencias no comparten sus repositorios de usuarios entre sí, ni tampoco con *Senasa Central*. Esto trae aparejado un gran número de inconvenientes al momento de compartir aplicaciones entre las distintas redes, como también a la hora de la administración de los recursos de TI y sistemas presentes.

A partir de aquí, el análisis hará foco en lograr esta tan ansiada "visión unificada de la organización" o las "partes del todo". Lo que haremos es ver, a partir de lo analizado en la sección que describe la situación actual, cuáles serían las maneras de obtener una unificación aceptable de la organización.

Lo primero en lo que nos ocuparemos es en analizar las posibles maneras que tenemos de unificar el repositorio de usuarios en un solo lugar, de manera de poder contar con la información actualizada en todo momento, sin tener que consultar varias bases de datos que contienen visiones parciales de la información de un usuario ó persona.

Es aquí cuando empiezan a aparecer las diferentes alternativas de solución, y en donde tenemos que iniciar los análisis de cada una de ellas para encontrar la que mejor se adapta al medio ambiente en el que nos encontramos. A continuación se hace un planteo de dichas alternativas, junto con un breve detalle de su correspondiente análisis.

ALTERNATIVA 1:

Despreocuparse por el tema y seguir manteniendo la misma estructura con la que se trabaja en la actualidad. Esta opción, si bien es poco ambiciosa no deja de ser una opción entre las disponibles en donde la complejidad del problema logra abrumar cualquier intento de plantear una solución. En este caso la tomamos como no viable, pues el constante crecimiento de la red de la organización así como las necesidades de integración de las distintas redes y dependencias que la conforman, nos llevan a tomar una decisión respecto a este tema. Además, luego de los análisis hasta acá realizados se es consciente de la existencia de una problemática, y por ende estamos de acuerdo en que el mismo debe ser abordado en el corto/mediano plazo.

ALTERNATIVA 2:

Solución mediante el uso de herramientas de software libre. Para el caso lo que se estudió, fue la posibilidad de emplear herramientas de software libre disponibles en el mercado que apuntaran a los problemas que se plantean. La idea sería emplear de alguna manera el Servicio de Directorio que contiene las credenciales empleadas para la validación a gran parte de las aplicaciones del Organismo (***LDAP senasa***), para unificar la validación de usuarios para el acceso al resto de los recursos. Es decir, y de acuerdo a como puede observarse a través de la figura 7, lograr que la validación de cualquier usuario a su PC de escritorio pueda ser realizada contra el LDAP ubicado físicamente en Casa Central.

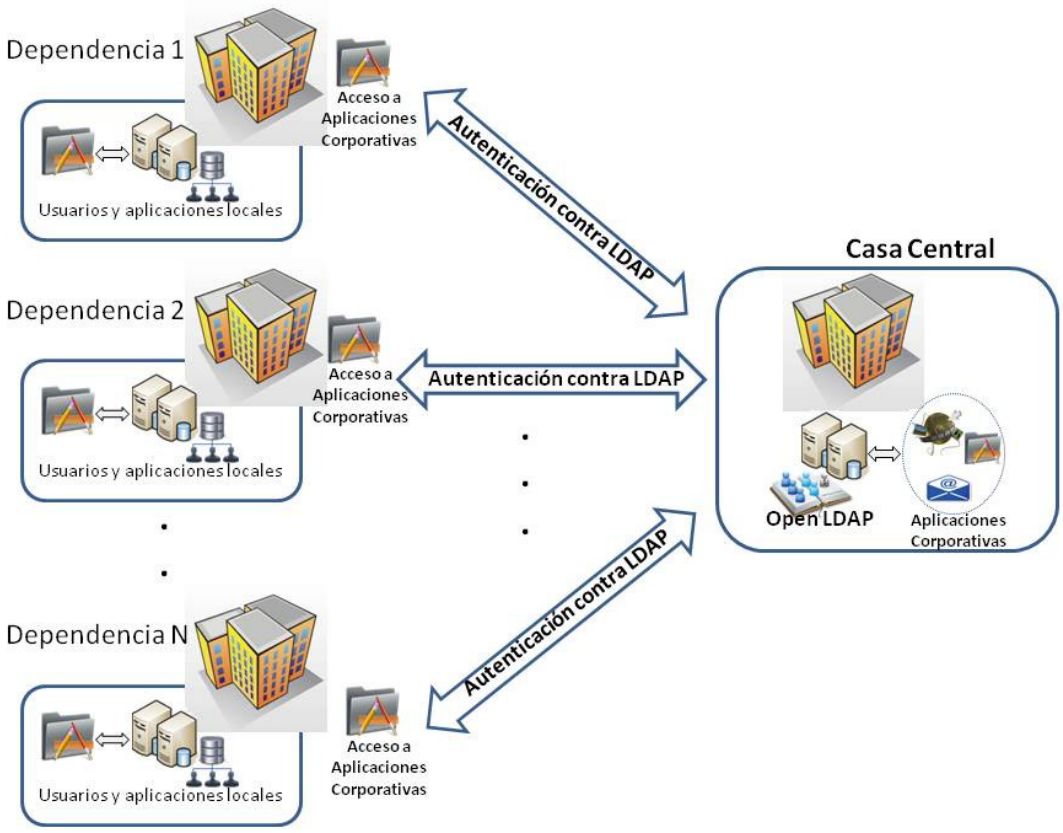


Figura 7: Open LDAP como repositorio de credenciales de usuario en todo el país

En ese sentido se evaluaron algunos productos observando también casos de éxito con soluciones de este tipo en el mercado. Se llegó a que una posible solución podría llegar a ser mantener repositorios de usuarios independientes para cada dependencia a través de servicios de tipo libre (por ejemplo alguna configuración particular de SAMBA:
OpenLDAP [26]**+Samba** [27])

Ventajas:

- Costos en licencias depreciable o nulo (Software libre)

- **IMPORTANTE:** La base de datos con todos los usuarios ya existe.

Desventajas:

- Difícil implementación.
- Costos en recursos humanos para la implementación.
- Solución muy a medida.
- Tiempo de análisis y pruebas.
- Complejidad en la administración y mantenimiento.
- Falta de experiencia en implementaciones similares.
- Si bien permite centralizar las credenciales de acceso a los recursos, no cuenta con la posibilidad de por ejemplo, la centralización de políticas de seguridad.
- Necesidad de contar con réplicas de la BD de LDAP (***LDAP senasa***) en cada una de las oficinas de tipo 1 de manera de minimizar la interrupción de servicios en caso de interrupción en los vínculos de red.
- Necesidad de una gran infraestructura edilicia en cada oficina en la que se implemente la solución:
  - Seguridad física
  - Aire Acondicionado
  - Energía eléctrica "segura"
  - UPS
  - Firewall

Podemos observar que esta alternativa presenta, a simple vista, un gran número de desventajas aunque cabe destacar que cuenta con ventajas y no menores. Una está relacionada con el costo económico, dado que a priori, no se necesita hacer una inversión inicial en software. A su vez, también se destaca la gran ventaja que es ya contar con una base de datos con la información de todos los usuarios del Organismo, que es la empleada para realizar la validación de credenciales a las aplicaciones y servicios corporativos. La información de dicha base de datos podría ser empleada en el caso de elegir esta alternativa.

Pero estas ventajas, pronto tienden a volverse despreciables si tenemos en cuenta que para llevar a cabo una implementación mediante esta alternativa, el ahorro en licencias de software se deberá invertir en recursos humanos altamente capacitados en las herramientas, y a su vez muy difícil de conseguir debido a la poca experiencia en el mercado de los recursos humanos en el tema y a lo puntual de la solución. A su vez se destaca que no se pudieron obtener ejemplos significativos de soluciones como esta en estructuras comparables a la de Senasa de manera de contar con casos de éxitos representativos que alentaran a la elección de esta alternativa.

ALTERNATIVA 3:

Implementación de Active Directory en todas las dependencias, permitiendo de alguna manera, la sincronización de los mismos con el ya existente en la red de *Senasa Central* (***ADS senasa***).

Ventajas:

- El sistema operativo posee muchas herramientas para facilitar la implementación.
- Mantenimiento más fácil.
- Posibilidad de manejar infinidad de facilidades de manera centralizada.
- Se reducen costos en la administración.
- La organización ya contaría con algunas licencias de software para ser empleadas.
- Es más sencillo encontrar recursos humanos capacitados en el tema.
- Se trata de una solución conocida y ampliamente utilizada [28].
- Integración con otras soluciones.
- Escalabilidad.
- Delegación de la administración.

Desventajas:

- Inversión inicial en licenciamiento de software.
- Falta de experiencia en implementaciones similares en el Organismo.
- Necesidad de una gran infraestructura de servidores (al menos dos servidores de relevancia para cada oficina).
- Necesidad de una gran infraestructura edilicia en cada oficina en la que se implemente la solución:
  - Seguridad física
  - Aire Acondicionado
  - Energía eléctrica “segura”
  - UPS
  - Firewall
- Complicaciones derivadas de la no existencia de personal capacitado en la solución en el interior.

Esta opción se presentó desde el primer momento como la más prometedora, y de hecho luego de llevar a cabo algunos análisis más profundos sobre la alternativa 2, se comenzó a trabajar más en detalle con esta como para tener más parámetros sobre las necesidades que se presentarían.

De la alternativa 3 se desprenden varias opciones a evaluar como disyuntivas de solución que se presentan como decisiones a ser tomadas. Es decir, que un análisis más detallado aún deriva a su vez varias posibles ramificaciones [29].

A) Dominio ÚNICO para todo el país. Representado a través de la figura 8. Esto significa extender el dominio ***ADS senasa*** de manera tal que el mismo incluya también al menos a todas las oficinas de tipo 1 del interior del país. En el caso del ejemplo representado a través de la figura 8, el nombre del dominio sería ***dominio.local***, y sería el mismo para todas las oficinas en las que se implemente. Esto significa que la base de datos de usuario es la misma para cada una de las oficinas que sean parte de dicho dominio, y a su vez, la misma se replicará de manera transparente a todas ellas.

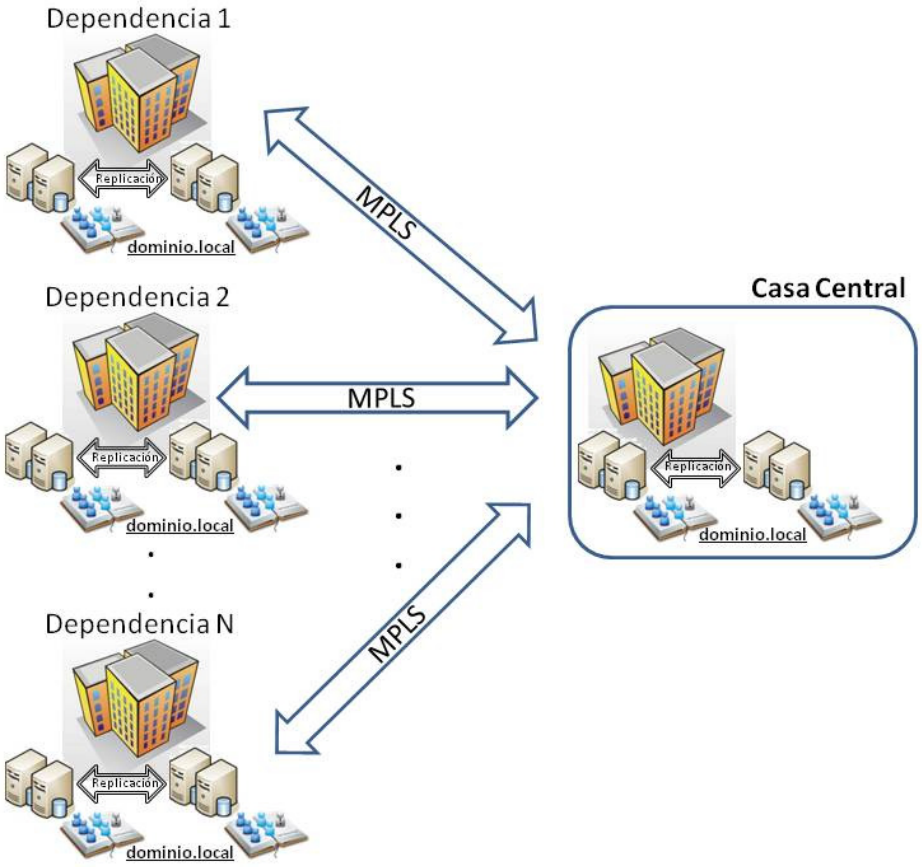


Figura 8: Dominio único en todo el país

Ventajas:

- Simplicidad en la administración, dado que hay una única base de datos (replicada).
- Introducción de gran número de nuevas funcionalidades deseadas.

- Administración centralizada del “país”: los cambios se replican de manera rápida al resto de las instancias de la base de datos de usuarios.
- Dado que cada oficina cuenta con una copia de la base de datos de usuario de manera local, en caso de caída del enlace que la vincula con Casa Central, seguiría funcionando sin notar cambios (excepto las aplicaciones corporativas que sólo existen en Casa Central). Una vez recuperado el enlace, se replicarían nuevamente las instancias de las bases de datos de usuarios.
- Fácil recuperación ante contingencia de un servidor cualquiera en una dependencia.
- La compartición de recursos se realiza de manera sencilla.

Desventajas:

- Dado que la base de datos de usuarios es única, cualquier error/accidente ocurrido sobre cualquier ocurrencia de la misma, se replicaría a todas las demás instancias.
- Necesidad imperiosa de contar con mecanismos fuertes de seguridad en cada uno de los lugares en donde se encuentre una réplica de la base de datos, teniendo en cuenta la criticidad de la información contenida.

B) Dominio central, y subdominios para cada dependencia. Representado a través de la figura 9. Se refiere a contar con un dominio principal en Casa Central (***ADS senasa*** en la figura con nombre ***dominio.local***) y subdominios distintos para cada una de las dependencias del interior (en la figura pueden observarse por ejemplo, ***subdom1.dominio.local***, ***subdom2.dominio.local*** y ***subdomN.dominio.local***). Esta estructura permite aplicar algunos parámetros de herencia desde el dominio padre a los distintos dominios hijo, pero a su vez, mantiene cierta independencia entre los hijos y su padre.

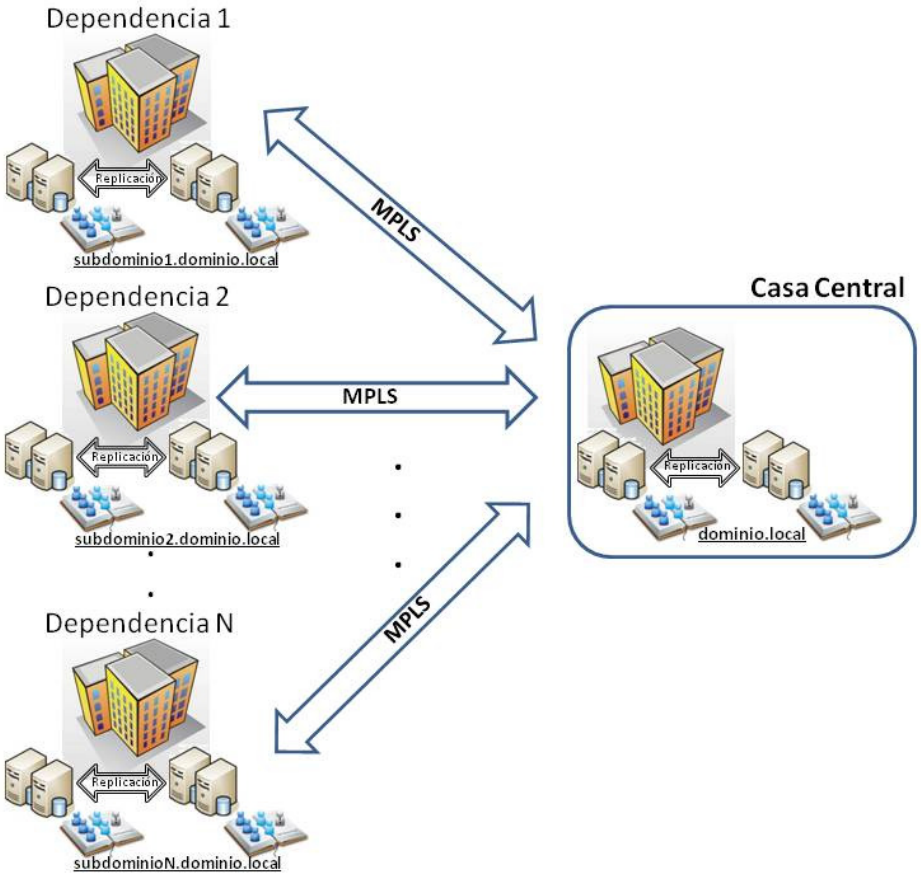


Figura 9: Dominio principal y subdominios

.

Ventajas:

- Dado que la base de datos de usuarios no es única, cualquier error/accidente ocurrido sobre cualquiera no repercutiría en mayor medida sobre las demás
- Introducción de gran número de nuevas funcionalidades deseadas.
- Dado que cada oficina cuenta con una base de datos de usuario de manera local, en caso de caída del enlace que la vincula con Casa Central, seguiría funcionando sin notar cambios.

Desventajas:

- La administración no sería tan simple como en el caso anterior, dado que ahora las bases de datos de usuarios son tantas como dominios haya.
- Administración descentralizada, lo cual lleva a contar con recursos humanos altamente capacitados para cada dependencia.

- La compartición de recursos entre distintos dominios/subdominio requiere algunas configuraciones.

C) Dominio central y dominios independientes relacionados entre sí a través de relaciones de confianza. Representado a través de la figura 10. Se refiere a que cada dependencia cuente con un dominio totalmente independiente de las demás. Aunque los mismos tendrían entre sí una relación de "confianza" la cual posibilitaría de alguna manera compartir recursos entre ellos.

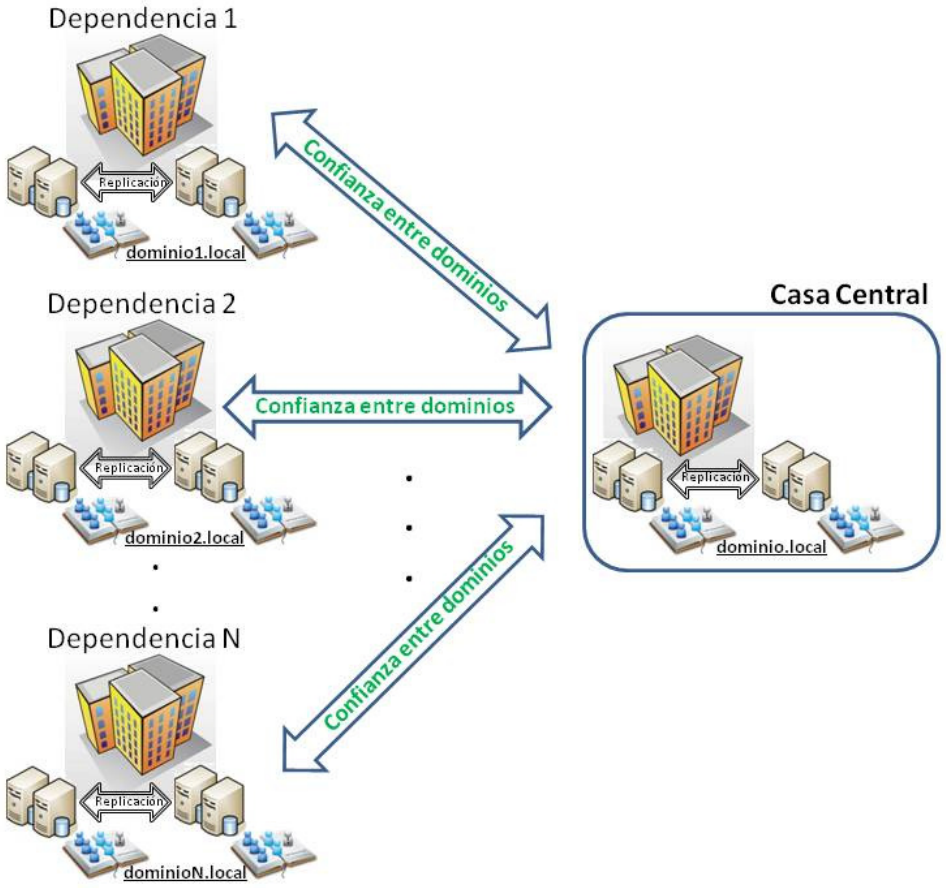


Figura 10: Dominios independientes relacionados a través de "confianza"

Ventajas:

- Dado que la base de datos de usuarios no es única, cualquier error/accidente ocurrido sobre cualquiera no repercutiría en mayor medida sobre las demás
- Introducción de gran número de nuevas funcionalidades deseadas.
- Dado que cada oficina cuenta con una base de datos de usuario de manera local, en caso de caída del enlace que la vincula con Casa Central, seguiría funcionando sin notar cambios.

Desventajas:

- La administración no sería tan simple como en el caso anterior, dado que ahora las bases de datos de usuarios son tantas como dominios haya.
- Administración descentralizada, lo cual lleva a contar con recursos humanos altamente capacitados para cada dependencia.
- La compartición de recursos entre distintos dominios/subdominio requiere algunas configuraciones.

D) **Implementación de un dominio central con sólo algunos dominios secundarios, subdominios o dominios independientes con otras redes compartiendo recursos a modo de grupo de trabajo.** Este caso contempla la posibilidad de combinar las tres opciones analizadas con anterioridad, y si bien es una alternativa posible la cual debe ser analizada como tal, es rápidamente descartada dado que la misma introduce algunas de las ventajas y todas las desventajas de las opciones anteriores. A su vez, convertiría la red en un entorno heterogéneo, complicado y difícil de entender. Por todo ello, no se realiza un mayor análisis.

5.1.2 Selección de alternativa: propuesta de solución

Visión unificada del Organismo

Hasta acá se hizo una introducción del escenario con el que se cuenta, y parte de la problemática a resolver. Llega el momento del análisis de las variables que inciden sobre el proceso de toma de decisiones, de manera tal de intentar seleccionar la "mejor" de las opciones disponibles.

Hasta aquí, se presentaron las distintas alternativas de solución al problema planteado, haciendo una breve enumeración de las principales ventajas y desventajas de cada una de ellas. A partir de ahora haremos hincapié en la propuesta elegida como solución, de manera de introducir los detalles relacionados a su implementación y así como también problemas secundarios presentados durante la misma.

La alternativa escogida es la número 3, es decir la que plantea la instalación de dominios Active Directory de MS Windows en todas las dependencias (en primera instancia sólo en aquellas que denominamos de tipo 1 que recordemos, serán la totalidad de las dependencias en algún momento). Es decir, unificar los repositorios distribuidos de usuarios en una "única" (más adelante veremos las razones de estas comillas) estructura organizacional. Pero tenemos que hacer la

aclaración que esta alternativa plantea a su vez, varias opciones posibles según se describiera oportunamente. Las mismas son:

A) Dominio ÚNICO para todo el país.
B) Dominio Central y subdominios para cada dependencia.
C) Dominio central y dominios independientes relacionados entre sí a través de relaciones de confianza.

Es aquí donde tendremos que hacer el análisis detallado del estado de situación particular del Organismo, de manera de seleccionar la opción que mejor se adecue a la realidad planteada. Y algunos de los puntos más importantes a tener en cuenta para tomar la decisión, se describen a continuación.

Aspectos a tener en cuenta para la toma de decisiones

Independientemente de la decisión que se tome entre los puntos anteriores hay que tener en cuenta varios aspectos más dado que la idea es introducir una solución, y no más problemas. Algunos de ellos se detallan como sigue:

- Configuración de cada una de las redes a integrar. Este punto incluye cantidad y tipo de aplicaciones, usuarios que las emplean, cantidad de equipos, servidores, etc.
- Ancho de banda de los vínculos que unen cada dependencia con *Senasa Central* y estabilidad de los mismos. Teniendo en cuenta que a través de los mismos, se realizarán todas las actividades relacionadas con la sincronización de bases de datos, y en algunos casos las que tiene que ver con los procesos de validación.
- Cantidad de tráfico que se necesita intercambiar para mantener las bases de datos de usuarios actualizadas y replicadas. Este punto está íntimamente relacionado con el punto anterior. Y se debe analizar el volumen de tráfico que hará falta para mantener toda la infraestructura funcional y "sincronizada".
- ¿Qué sucede si un enlace permanece inactivo por un tiempo determinado? ¿La dependencia puede seguir operando? ¿Podrá volver a recuperar el sincronismo de una manera sencilla? ¿Podría haber pérdida de información o de integridad en la misma?
- Tipo de aplicaciones existentes en cada red, como también la plataforma sobre las que se encuentran implementadas (Windows, Linux). Este punto nos facilitaría bastante la toma de decisiones teniendo en cuenta que en las primeras dependencias de tipo 1 a integrar, los sistemas operativos tanto de las terminales de usuario como de los servidores presentes coincidían en ser todos de tipo MS Windows.
- Cantidad de usuarios en cada una de las redes a integrar. Este punto nos permitirá considerar la posibilidad de tener o no servidores locales en las dependencias y a su vez, generó la necesidad de incorporar personal informático capacitado en algunas dependencias del interior.

- Condiciones de seguridad (tanto física como lógica) presentes en cada dependencia. Es necesario considerar dónde residirán los equipos servidores, teniendo en cuenta la posibilidad que los mismos contengan información crítica (presencia de aires acondicionados, ups, energía segura y estable, firewall, etc). Esta es una condición determinante para la implementación. Dado que de no contar con los mínimos requisitos de seguridad dentro de la estructura edilicia, se descarta la dependencia como objetivo. Lo que ha sucedido en todos los casos, es que todas las dependencias han realizado las reformas correspondientes dentro de su infraestructura edilicia, de manera de adecuarse a las necesidades planteadas y poder contar con equipamiento informático más avanzado, servidores, switchs, firewall, etc.
- Dinamismo de los ambientes de producción. Este punto está relacionado con la cantidad de modificaciones en el ambiente de producción que se pudieran llegar a producir. Por ejemplo altas, bajas y modificaciones de usuarios, equipos, aplicaciones, etc. de manera de considerar aspectos que luego estarán relacionados con las replicación de los mismos en los repositorios que sea necesario. Está claro que no es lo mismo un ambiente muy dinámico, teniendo en cuenta que cada vez que se realiza una modificación, necesitamos que la misma se replique al resto de la infraestructura, que un ambiente estable sin muchas variaciones que requerirá de replicaciones quizás más esporádicas.
- Aspectos relacionados con la política, de tipo organizacionales o bien restricciones de tipo legal. Estos aspectos tendrán que ver con la manera en que cada una de las dependencias se administrará así como también con la posibilidad de que las mismas sean independientes entre sí, o puedan formar parte de una estructura lógica única. En muchos casos estos aspectos tienen que ver con decisiones de la política de la organización y no con las mejores soluciones técnicas. Por suerte en el caso del trabajo que se describe aquí, sólo se tuvieron escollos de tipo técnico.
- Cantidad de recursos humanos capacitados para poder mantener la estructura funcional en el tiempo. ¿Hay un administrador disponible en cada una de las redes? En la gran mayoría de los casos la respuesta es no. Se cuenta con personal que efectúa tareas relacionadas con el Soporte técnico, pero no con la administración de equipos tipo servidores. En algunos casos la persona afectada a este tipo de roles, se encuentra a cientos de kilómetros de la oficina a la que da soporte. Este punto fue de vital importancia a la hora de determinar aspectos relacionados con la distribución de equipamiento, y alternativa de solución, dado que con este marco la mejor alternativa es mantener una infraestructura lo más uniforme posible, distribuida, pero tratando de manejarla de manera centralizada.
- Modalidad en la que se lleva a cabo la administración de las dependencias. Relacionado con el ítem anterior.
    - ¿La misma se realiza de manera descentralizada? ¿Cada red tiene un responsable que responde por ella y que toma decisiones por ella a nivel local?

    - Centralizada. Donde cada dependencia es administrada de manera centralizada por personal de *Senasa Central* y no tiene la potestad de decidir aspectos relacionados con la configuración de la infraestructura tecnológica.
- Limitaciones de tipo geográficas. Este aspecto tiene que ver con los vínculos que unen las dependencias con *Senasa Central* lo cual tendrá mucha incidencia a la hora de tomar decisiones sobre la estructura que se implemente.
- Consideraciones relacionadas al espacio de nombres DNS[24]. Aspectos como los espacios empleados por cada una de las dependencias de manera interna o para publicar servicios en la red pública. Si bien no se hará hincapié en este punto, cabe destacar que al momento de iniciados los trabajos el servicio de DNS si bien en todos los casos es de vital importancia para el funcionamiento de cualquier infraestructura de TI, no era un servicio que se pudiera llegar a considerar como fundamental. A partir de la introducción de esta estructura de distribuida, el servicio DNS se ha convertido en la piedra fundamental de la misma, siendo su correcto funcionamiento una condición por demás necesaria para que la misma opere de manera adecuada.
- Presencia de políticas de algún tipo (por ejemplo de contraseñas) a nivel local. Teniendo en cuenta que lo que se desea es manejar este tipo de políticas de manera centralizada, la presencia de definiciones de manera local en las dependencias, dificultaría el crecimiento de la infraestructura.
- Equipamiento actual de la organización, equipamiento necesario para llevar a cabo la implementación, perspectiva de crecimiento a mediano y largo plazo. Este punto es otro de los que se destaca como de vital importancia para la implementación, teniendo en cuenta que mucho del equipamiento empleado para la solución, ya era parte del inventario del Organismo, lo cual facilitó mucho la toma de diversas soluciones. A su vez, asumiendo la modificación de todas las dependencias de tipo 2 para pasar a ser parte de la solución como dependencias de tipo 1, generará la necesidad de adquirir un gran volumen de equipamiento nuevo.
- La movilidad de los usuarios de una dependencia a otra, ¿es determinante? La respuesta es SI en un gran número de casos. La dispersión geográfica del Organismo, y las diversas tareas efectuadas por los agentes del mismo hacen que sea necesario que un usuario que hoy accede a los recursos desde Casa Central, cuente con la posibilidad de realizarlo mañana desde cualquier otra dependencia. Este aspecto se verá facilitado a partir de los cambios analizados e introducidos a partir de la solución aquí planteada.
- ¿Es factible contar con la infraestructura adecuada en cada una de las oficinas? Por suerte la respuesta es afirmativa en la mayoría de los casos analizados al momento.
- Servidores, UPS, Aire acondicionado, seguridad física, energía confiable, firewalls, dispositivos para realizar backups, etc.
- ¿Qué volumen de información manejan las oficinas?
- ¿Es necesario que las oficinas compartan información/datos entre sí?

[24] *Ver **Glosario** al final del documento*

- ¿Es necesario contar con la posibilidad de implementar políticas a nivel global de toda la infraestructura del Organismo? ¿Es este un factor determinante?
- ¿Se prevé un crecimiento en la actual infraestructura? Como ya se mencionara este punto no es anecdótico sino primordial. Se prevé la incorporación de más de 450 dependencias a la infraestructura (hoy dependencias tipo 2) lo cual hace tener en cuenta muchos aspectos relacionados al crecimiento de la misma.

Sin duda los factores que inciden sobre la decisión a tomar son varios, y no es para menos si tenemos en cuenta que lo que se está evaluando, es la forma en la que la infraestructura física de un Organismo de más de 6000 empleados funcionará de aquí en adelante. Sin mencionar que un fracaso en la implementación, podría llegar a tener consecuencias drásticas teniendo en cuenta que la misma tiene un gran impacto sobre toda estructura informática del Organismo.

Sin entrar en detalle de lo evaluado para cada uno de los aspectos antes listados, sino teniendo en cuenta sólo aquellos con más peso en el proceso decisivo, se llega a la conclusión que la mejor de las alternativas de implementación de Active Directory para las dependencias de tipo 1 de Senasa, es la de un único dominio para todo el país. Es decir, que gráficamente a lo que se apunta es a algo como lo que se ilustró con anterioridad en la figura 8. Lo que se hace es extender el dominio ***ADS senasa*** en todas las oficinas de tipo 1, de manera tal que la base de datos de usuario almacenada en ese servicio de directorio sea única y se replique en cada una de esas oficinas.

De esta manera cualquier agente de Senasa que forme parte de ***ADS senasa***, podría hacer uso de cualquier tipo de recurso más allá del a ubicación geográfica que dicho recurso tenga en el país (siempre y cuando los permisos para llevar a cabo dicho uso lo permitan). Esto es así, pues dicha persona tendría credenciales disponibles en ese único repositorio replicado, y a través del mismo podría convertirse en un usuario móvil.

Beneficios

Si bien ya se destacaron algunos de los beneficios que se obtendrían a partir de esta nueva implementación, considero oportuno hacer mención de alguno de ellos detallando algo más sobre los mismos.

- Tolerancia a fallas (dado que en las redes locales se instalarían al menos un repositorio de credenciales o dos dependiendo de diversos factores)

- Flexibilidad tanto para la implementación de las necesidades actuales como para futuras expansiones.

- Administración centralizada de los recursos. Ideal para el entorno descripto en donde no se cuenta con personal capacitado en cada una de las dependencias.

- Replicación tipo multi master. Es decir que las modificaciones se pueden llevar a cabo en cualquiera de las oficinas que forman parte de la infraestructura, y aún así serán replicadas al resto de las dependencias.

- Sincronización horaria en toda la red. Esta configuración facilita notablemente la configuración de los equipos para que los mismos sincronicen la hora a través del protocolo ntp[25] (*Network Time Protocol* en inglés ó *Protocolo de Hora de Red* en castellano). De esta manera se logra que tanto servidores, como cada terminal de usuario, firewalls, switchs, UPSs y demás equipamiento cuente con la misma hora.

- Definición única de directivas de grupo para todas las redes involucradas.

    - Cada red cuenta con una instancia local de un servidor de actualizaciones de seguridad.

    - Directivas de contraseña.

    - Configuración automática de ciertos parámetros de las terminales de usuario de manera centralizada.

- Simplificación en la definición de repositorios centralizados de información (servicio de archivos, aplicaciones existentes y futuras).

- Facilita la compartición de datos e información entre las distintas redes del organismo.

- Permite la movilidad de las personas. Esto significa que la persona empleará siempre las mismas credenciales de usuario independientemente de si está accediendo a la red corporativa desde una terminal ubicada en Comodoro Rivadavia, que si lo hace desde una en Jujuy.

Infraestructura física de la solución

A través de la figura 11, se observa cómo es la infraestructura de servidores y hardware en general resultante en cada una de las dependencias de tipo 1 sobre la que se llevaría a cabo la implementación hasta aquí descripta. A su vez, puede visualizarse también la nueva infraestructura de servicios a prestar dentro de las dependencias. Servicios muchos de los cuales no eran prestados o bien por la misma complejidad por la ausencia de una configuración amigable como la que se introduce, o bien por falencias de hardware. Estos, colaboraron en mucho al ordenamiento de las oficinas y a su vez, facilitaron en gran medida tareas tales como la administración remota desde Senasa Central como también tareas relacionadas con la continuidad del servicio.

[25] *Ver **Glosario** al final del documento*

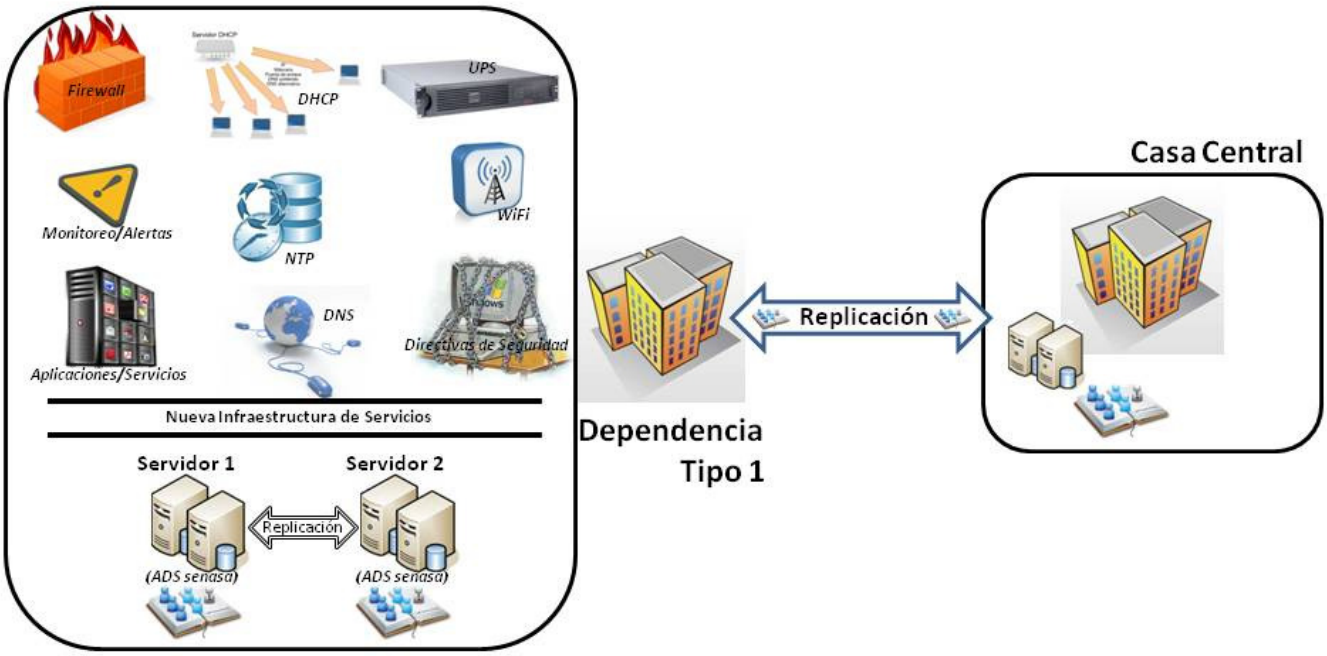


Figura 11: Configuración de cada dependencia de tipo 1

Es decir que para la implementación, se requieren al menos dos servidores físicos en donde se instalarían dos controladores de dominio de ***ADS senasa***. Esto nos permitirá lograr continuidad de servicio en el caso que alguno de ellos sufriera algún desperfecto. A su vez, en caso de caída del enlace de red que vincula la dependencia con Senasa Central, el servicio tampoco se vería interrumpido dado que la base de datos de usuario también se encuentra dentro de las instalaciones de la dependencia (excepto para aquellas aplicaciones/sistemas corporativos que sólo se brindan desde *Senasa Central*, los cuales permanecerán inaccesibles hasta la reposición del vínculo de red). También podemos observar a través de la ilustración, que cualquier modificación que se realice en la base de datos de usuario, ya sea dentro del ámbito de la dependencia, o bien en Casa Central, se replicará a través del vínculo de red.

Conclusiones

Lo que hemos logrado hasta aquí es homogeneizar para todas las dependencias de tipo 1, las credenciales empleadas para por ejemplo, el inicio de sesión interactivo a las PCs de usuario. Si bien este no es el único beneficio obtenido, también tenemos que destacar que vemos aumentada y en mucho, la complejidad de nuestra infraestructura de red, dado que para cada una de las dependencias se introdujo al menos dos servidores (sin mencionar el resto de los dispositivos

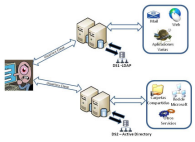
ilustrados a través de la figura 11). Esto se ve justificado ampliamente con la gran variedad de nuevos servicios introducidos en las dependencias de tipo 1.

Pero esto no soluciona la totalidad del problema en lo que respecta a validación de credenciales de usuario para el acceso a recursos del Organismo, dado que tenemos que recordar que ya al inicio del análisis, se había mencionado que además del servicio de directorio ***ADS senasa***, también se contaba con un segundo servicio de directorio implementado con herramientas de software libre, al cual habíamos denominado ***LDAP senasa***. Contra este último, se lleva a cabo la autenticación de muchas de las aplicaciones/servicios corporativos, y es allí, en el único repositorio en donde se encuentran almacenados la totalidad de los usuarios de Senasa.

Entonces, si bien obtuvimos grandes beneficios mediante la incorporación de ***ADS senasa*** en todas las dependencias de tipo 1, aún contamos con el "problema" de contar con dos grandes repositorios de usuarios disjuntos entres sí: ***ADS senasa*** y ***LDAP senasa***.

A partir de la sección siguiente, se inicia el análisis para abordar esta segunda problemática, y se detallan los aspectos relacionados a la misma.

5.2 Punto 2: Dos grandes repositorios de usuarios disjuntos



Introducción

Luego de realizada la descripción de alternativas al problema de la visión disgregada del Organismo introducida por la no existencia de centralización de credenciales, analizadas las posibles soluciones y seleccionada la alternativa a emplear, surge una nueva problemática producto justamente de dicha selección. Esto es porque el abordaje de la mejor solución para el punto anterior introduce una nueva problemática no menor. Aunque cabe destacar que la problemática que se analiza en este apartado, si bien ya existía previo a la selección de alternativa de solución al *"Punto 1: Visión disgregada del Organismo"*, la misma se vio acentuada y la necesidad de abordar el problema como tal quedó en manifiesto.

Decíamos que el problema de los grandes repositorios de usuarios ya existía previo a la selección de la alternativa en el punto anterior, y esto es cierto. Recordemos que al iniciar las descripciones de la infraestructura del Organismo, destacamos la presencia de un Servicio de Directorio (no completo) existente en Casa Central e implementado a través de la herramienta de Microsoft Active Directory (***ADS senasa***). Y a su vez, también se habló del otro Servicio de Directorio implementado a través de la herramienta de software libre OpenLDAP (***LDAP senasa***) para realizar la autenticación de la mayoría de las aplicaciones del Organismo. Como decíamos, luego del análisis del punto anterior, se concluyó que la mejor solución era hacer crecer ***ADS senasa*** hasta extenderlo a todo el país. Teniendo en cuenta que el OpenLDAP ya se encontraba

prestando servicios en todo el país (con la salvedad que este último sólo reside en Casa Central), es donde nos surge la necesidad de abordar un nuevo problema: *Hacer coexistir a estos dos grandes repositorios de credenciales disjuntas, sin nexos de sincronización ni relación aparente entre sí*.

Quizás a simple vista el problema planteado como "Punto 2" pueda no ser tomado como un problema en sí mismo. Teniendo en cuenta que tenemos dos grandes repositorios de usuarios disjuntos, en donde cada uno de ellos es empleado de manera bien definida para distintos tipos de aplicaciones/servicios presentes en el Organismo, podríamos concluir que es esa la metodología de trabajo en el Organismo, y definir cada aplicación/servicio con su repositorio de credenciales asociado. Pero es aquí en donde surge el rol del profesional informático, en donde plantea mejorar el entorno de trabajo a través de herramientas más puntuales, y mejores configuraciones de las herramientas existentes para hacer que todas las componentes que hacen a una solución, logren de la mejor manera su fin que es ni más ni menos que "Simplificar la vida al usuario" tomando por usuario tanto a la persona que accede un servicio particular, como el administrador que tiene el rol de hacer que las componentes interactúen entre sí.

Entonces, y teniendo en cuenta lo anterior como premisa, es aquí donde nos encontramos con la necesidad de abordar el "Punto 2" como un problema para obtener la solución que mejor se adecue a las falencias planteadas.

Iniciaremos de esta manera el análisis del otro gran problema existente, que mantiene estrecha relación con el punto anterior. Hasta se podría decir que son los dos partes de un único problema, pero para facilitar el análisis, y plantear mejor las opciones de solución, se decidió separarlos en dos ítems distintos, y analizarlos de manera independiente para luego si obtener una visión macro del asunto como solución integral.

Este tema, quedó planteado ya en secciones anteriores (Figura 5) en donde se mostraban los dos grandes repositorios ó bases de datos conteniendo credenciales de usuarios. La primera empleada para la validación de aplicaciones y desarrollos, y la segunda para el acceso a la red del Organismo, los recursos compartidos y otros servicios de la red de Active Directory. Lo malo de esto, es que en ningún momento las credenciales de ambas bases de datos tienen algún tipo de sincronismo entre sí, es decir, son totalmente disjuntas y no relacionadas. Esto significa que una misma persona podría tranquilamente tener distintos "nombres de usuario" en cada base de datos, sin meternos obviamente en la inexistencia de procesos para lograr que la contraseña coincida.

Como conclusión, cada usuario debe recordar más de un par de "nombre de usuario y contraseña" y no sólo eso, también debe recordar para qué situaciones debe emplear una u otra lo cual es en algunas circunstancias, otro tema en sí mismo.

Un dato no menor para destacar en este nuevo apartado, tiene que ver con los nombres de usuario de uno y otro repositorio. Si bien se mencionó que estos dos repositorios funcionan de manera independiente entre sí, sin mantener ningún tipo de sincronismo se debe decir también

que los nombres de usuario coinciden en ambos repositorios. Esto significa que si una persona llegara a contar con usuario en ambos repositorios, entonces esos usuarios coincidirían (refiriéndonos al nombre de usuario empleado para validar) no necesariamente las claves, siendo esto último una decisión personal de cada persona.

5.2.1 Alternativas de solución

A partir de acá, y teniendo como alternativa seleccionada del "Punto 1" la alternativa 3 en donde se hizo la extensión del dominio de Active Directory[26] de Casa Central a todas las oficinas (de tipo 1) del país, se inicia el proceso de análisis de opciones para obtener la mejor solución a la existencia de multiplicidad de credenciales de usuario.

Luego de evaluar las alternativas de solución posibles, se distinguen como viables las que a continuación se analizan:

ALTERNATIVA 1:

Sincronizar las credenciales entre AD y LDAP (o sea entre ***ADS senasa*** y ***LDAP senasa***) mediante algún procedimiento. Esta alternativa consiste en que cada persona cuente con un usuario en cada uno de los repositorios con exactamente el mismo *username*. Luego, introducir software para que al momento de cambiar la contraseña en cualquiera de los dos repositorios, la misma sea "capturada" y enviada al otro repositorio de manera tal que la clave sea siempre la misma en los dos repositorios. Cabe aclarar que el usuario podría llegar a cambiar la clave desde aplicaciones/servicios que validan o bien contra el servicio de directorio de LDAP, o bien contra el servicio de directorio de Active Directory. Esto significa que habría que implementar los mecanismos para capturar y sincronizar las claves para ambos casos. Esto se ve ilustrado en la figura 12 en donde el usuario inicia el proceso de cambio de clave desde una aplicación ó servicio que autentica contra el repositorio de LDAP. En este caso, se puede observar que el proceso de sincronización de claves (PassSync en la ilustración) se coloca en el medio para capturar y enviar la clave al otro repositorio antes que la misma se almacenada de manera cifrada e ilegible dentro de su base de datos.

[26] *Ver **Glosario** al final del documento*

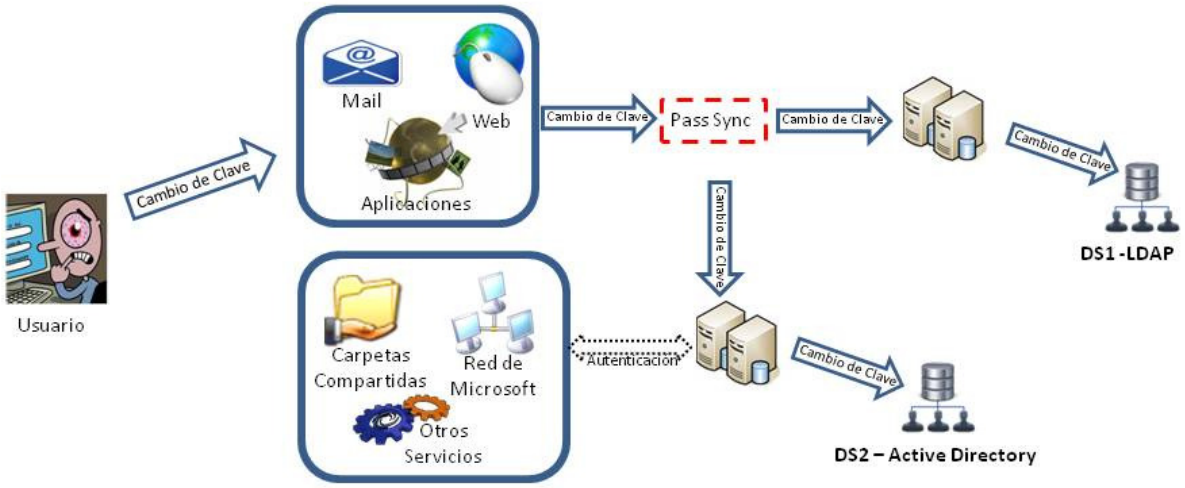


Figura 12: El usuario cambia su clave desde una aplicación ó servicio autenticado en LDAP

De igual manera en la figura 13 se puede observar cómo el usuario inicia el proceso de modificación de clave a través de alguna aplicación/servicio que autentica contra el repositorio de Active Directory, y cómo de manera similar que lo descripto para la figura anterior, el proceso PassSync captura y envía la clave al LDAP antes que Active Directory la almacene de manera cifrada e ilegible dentro de su base de datos.

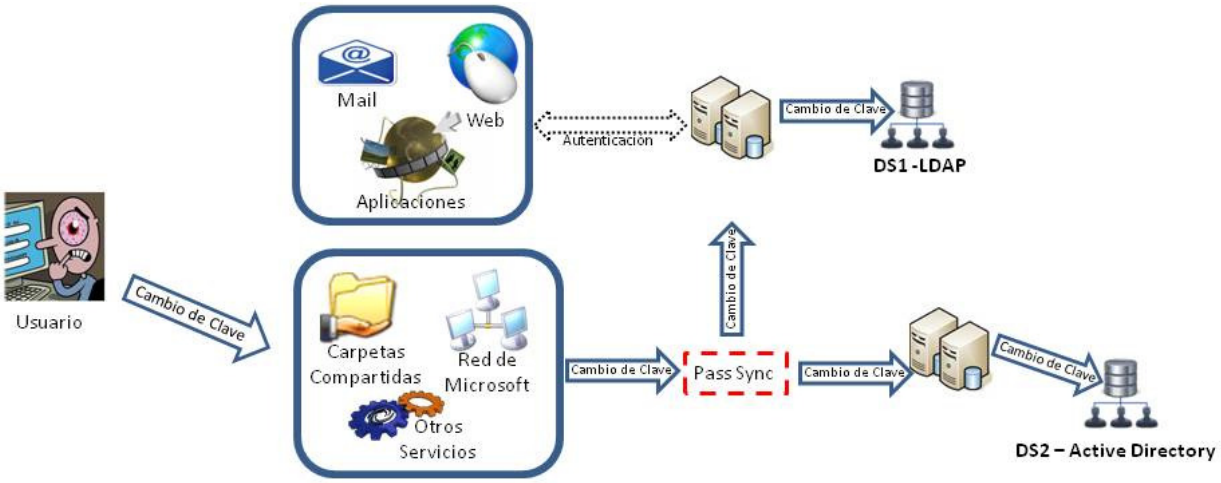


Figura 13: El usuario cambia su clave desde una aplicación ó servicio autenticado en Active Directory

De esta manera estaríamos logrando que si bien el usuario podría no ser único (podría tener al menos una ocurrencia en cada servicio de directorio) el mismo tendría la misma clave en

ambos repositorios lo cual daría a la persona que lo emplea, la sensación de estar empleando un único par usuario-contraseña para todos los servicios y aplicaciones de la red, ya sea local o corporativo.

Ventajas:

- Evita abordar la problemática de consolidación, dado que los repositorios se mantendrían de manera independiente entre sí, pero vinculados con un sincronismo en las claves de los usuarios.

Desventajas:

- Se rompe el sincronismo fácilmente y es difícil volver al estado de "sincronizado". Esto sería difícil de solucionar.
- Complejo llevar a cabo la sincronización inicial
- No hay muchas opciones en el mercado para su implementación.
- Siempre se tendrán dos repositorios distintos con todo lo que ello implica.

ALTERNATIVA 2:

Implementación de un producto de *metadirectorio*[27]. En esta alternativa seguirían existiendo los dos servicios de directorios en cuestión y se colocaría un objeto más dentro del proceso de validación de credenciales de usuario denominado justamente metadirectorio. La función del mismo es determinar a qué repositorio de usuarios consultar de acuerdo a cada petición de validación. Esta determinación se lleva a cabo de acuerdo a reglas definidas dentro del metadirectorio. En este caso, se podría llegar a dar que exista un mismo usuario para la persona "Juan Perez" con nombre de usuario jperez en ambos directorios, y dependiendo a la aplicación/servicio al que el usuario requiera ingresar, se podría validar contra uno o el otro.

[27] *Ver **Glosario** al final del documento*

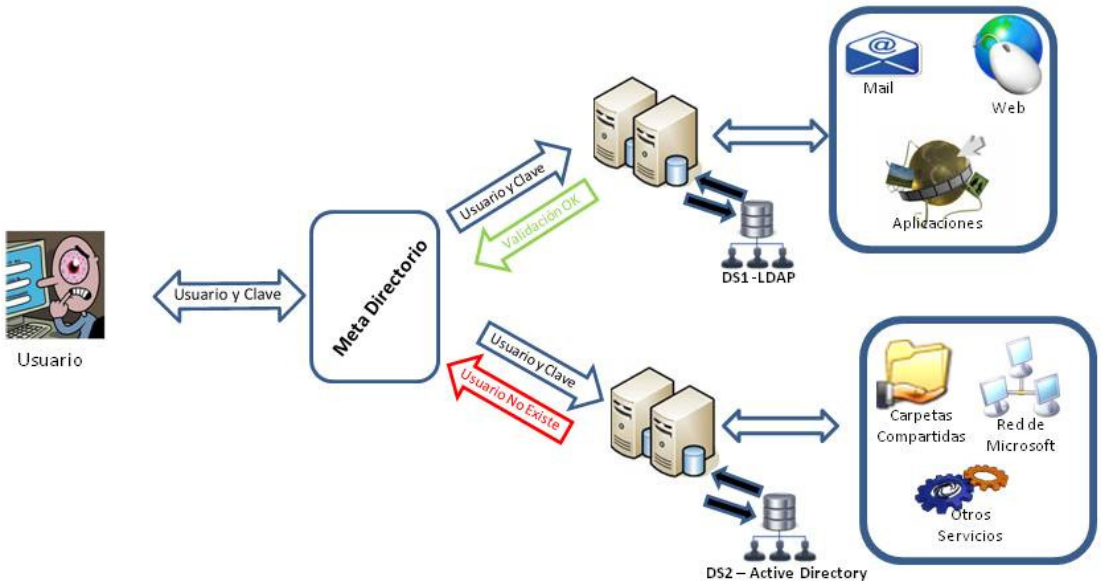


Figura 14: Solución a través de un metadirectorio.

Ventajas:

- Ampliamente empleada en el mercado

Desventajas:

- Alto costo de licenciamiento de software (Aunque se podría implementar con herramientas de código abierto, la solución se tornaría demasiado compleja dejando una sensación de cierta "inestabilidad")
- Complejo llevar a cabo la sincronización inicial

ALTERNATIVA 3:

Unificar ambos directorio dentro del servicio de Active Directory. Es decir migrar todos los usuarios que estuvieran dentro de ***LDAP senasa*** al ***ADS senasa***, y de esta manera obtener un gran servicio de directorio con bases en el servicio de Active Directory. Como se puede ver a través de la figura 15 toda la verificación de credenciales se lleva a cabo contra un único repositorio implementado a través de Active Directory. Y este, es quien autoriza o no el acceso a todas las aplicaciones y servicios brindados desde el Organismo.

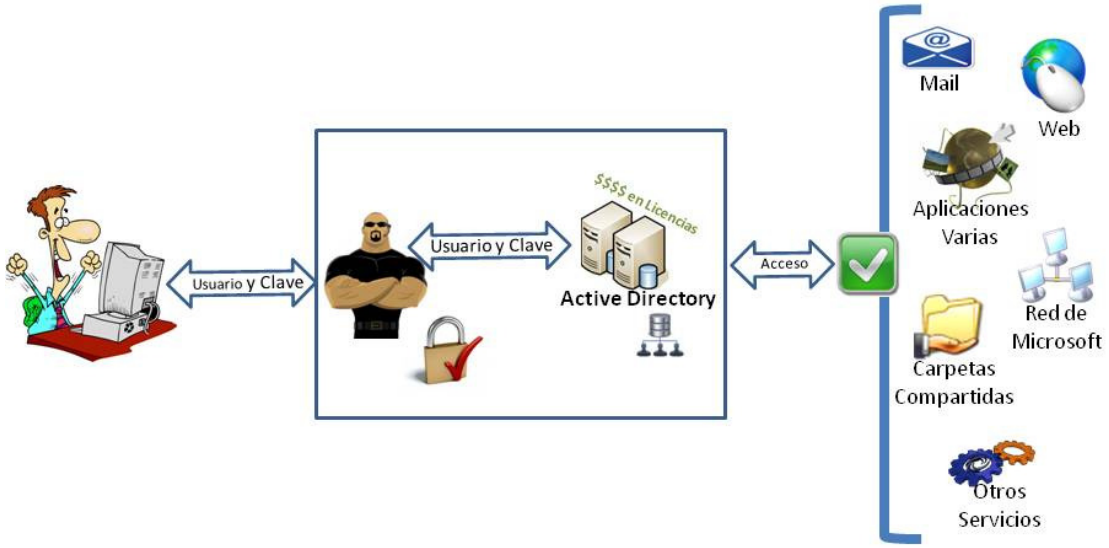


Figura 15: Unificar las bases de datos de usuarios empleando Active Directory

Ventajas:

- Simplicidad.
- Convergencia rápida.
- Requiere de poco análisis.
- Conocimiento de la herramienta.

Desventajas:

- Costo extremadamente alto en licencias de software por usuario, dado que cada usuario que se crea dentro del servicio de Active Directory tiene un costo en licencia. Y para este caso, todos los usuarios que sean migrados desde el LDAP, sólo usarían la validación de credenciales contra AD, y no todas los beneficios para los que AD ha sido concebido. No entraré en más detalles con este tema, pero es esta desventaja la que me llevó a descartar esta opción, aún siendo la que a primera vista más se ajustaba a las necesidades planteadas en cuanto a simplicidad y velocidad de su implementación. ***ADS senasa*** cuenta con unas 2000 cuentas de usuario, mientras que ***LDAP senasa*** cuenta con unas 6000 cuentas. Esas 4000 cuentas que las diferencian, deberían ser migradas desde ***LDAP senasa*** hacia ***ADS senasa***, lo cual nos llevaría a tener que pagar licencias por un directorio de 6000 cuentas, teniendo en cuenta que sólo 2000 de ellas emplearán los grandes beneficios provistos por AD (validación de la estación de trabajo, aplicación de políticas de seguridad y tantas otras que ya se analizaran en este trabajo). Aún cuando

se estime que en un futuro todas las oficinas formarán parte de esta nueva estructura.

- Además de lo expuesto en el punto anterior, esto empeoraría teniendo en cuenta la perspectiva de crecimiento que se posee en cuanto a cantidad de usuarios hacia el futuro. Usuarios en gran medida externos al Organismo, que sólo necesitan una credencial para validarse con alguna aplicación puntual, configuración que hace que no amerite pagar una licencia de Active Directory para ello.

ALTERNATIVA 4:

Implementación a través de una herramienta de Microsoft denominada AD LDS [30]

Ventajas:

- No insume un costo extra en licenciamiento de software, o bien el mismo es mínimo.
- Elimina los costos de licencias de usuario de Active Directory que se explicaran como desventaja en la Alternativa 3.
- Permite una alta integración en lo que respecta a implementación de políticas de seguridad de manera centralizada, así como otras tantas bondades en este sentido.

Desventajas:

- Complejo llevar a cabo la sincronización inicial
- Desconocimiento de la herramienta.

En este párrafo no se hará más énfasis en esta opción, dado que es la alternativa elegida como solución, y será en la próxima sección en donde se haga un análisis más detallado de la misma, haciendo hincapié en pormenores de los beneficios obtenidos con su implementación así como también en las dificultades introducidas.

5.2.2 Selección de alternativa: propuesta de solución

Único repositorio de usuarios para todo el Organismo

Como se contara con anterioridad, si bien se lograron unificar las credenciales de usuario para el acceso a los servicios de todas las oficinas de tipo 1 a través de la implementación del servicios de Directorio Active Directory, surge la problemática de contar ahora con dos servicios de

directorio disjuntos (***ADS senasa*** y ***LDAP senasa***). El desafío ahora, es lograr unificarlos en uno o bien lograr que la validación de usuarios se realice de manera transparente simulando o haciendo creer a las personas que la base de datos contra la que se validan sus datos es única y centralizada. Para ello, analizamos las alternativas en los párrafos anteriores, y es este el momento de hacer la selección de la que he considerado en el presente trabajo como la que mejor se adecua a las necesidades presentadas.

La solución planteada como alternativa y elegida como tal se obtiene a través de un producto de software comercial de la empresa Microsoft denominado AD LDS (Active Directory Lightweight Directory Service)[28] .Dicho producto presenta las bondades de un servicio de LDAP interno integrado, con el agregado de una interacción natural y armoniosa con el servicio de Directorio Active Directory (ello se debe sin duda a la compatibilidad esperable de los productos de la empresa Microsoft). El presente trabajo no tiene por finalidad hacer una reseña detallada del producto en sí que se ha elegido como herramienta a implementar, sino que la meta es hacer hincapié en las características que la misma posee para cubrir la/las problemáticas planteadas.

Quizás al lector le surjan algunas preguntas de manera natural, como de igual manera me surgieron al momento de analizar cada una de las propuestas y de realizar las pruebas iniciales con las herramientas seleccionadas. Algunas de ellas son:

- ¿Qué beneficios obtengo mediante la incorporación de esta nueva herramienta de software?
- ¿Por qué incorporar un nuevo producto corporativo y licenciado de software cuando tengo un LDAP de tipo open source y sin limitaciones?
- ¿No es esta una solución de iguales características a la ofrecida por un metadirectorio de las que ya se hicieran mención antes?

Las respuestas a estas preguntas si bien no son sencillas, pueden ser explicadas con brevedad y sencillez al decir que la herramienta AD LDS, posee mecanismos de interacción bien marcados, definidos entre un servicio de LDAP y el Active Directory propiamente dicho que nos proveerán una gran variedad de posibilidades. Estas posibilidades y facilidades brindadas, quizás queden más a la luz cuando en los párrafos que siguen, se explique con mayor nivel de detalle aspectos relacionados a la solución.

La estructura de la solución, y los beneficios logrados mediante la incorporación de esta nueva herramienta de software, se ilustran a través de la figura 16 en donde se puede visualizar cómo interactúa cada una de las componentes involucradas.

[28] *Ver **Anexo II**: "Active Directory Lightweight Directory Service (AD LDS)" para más información.*

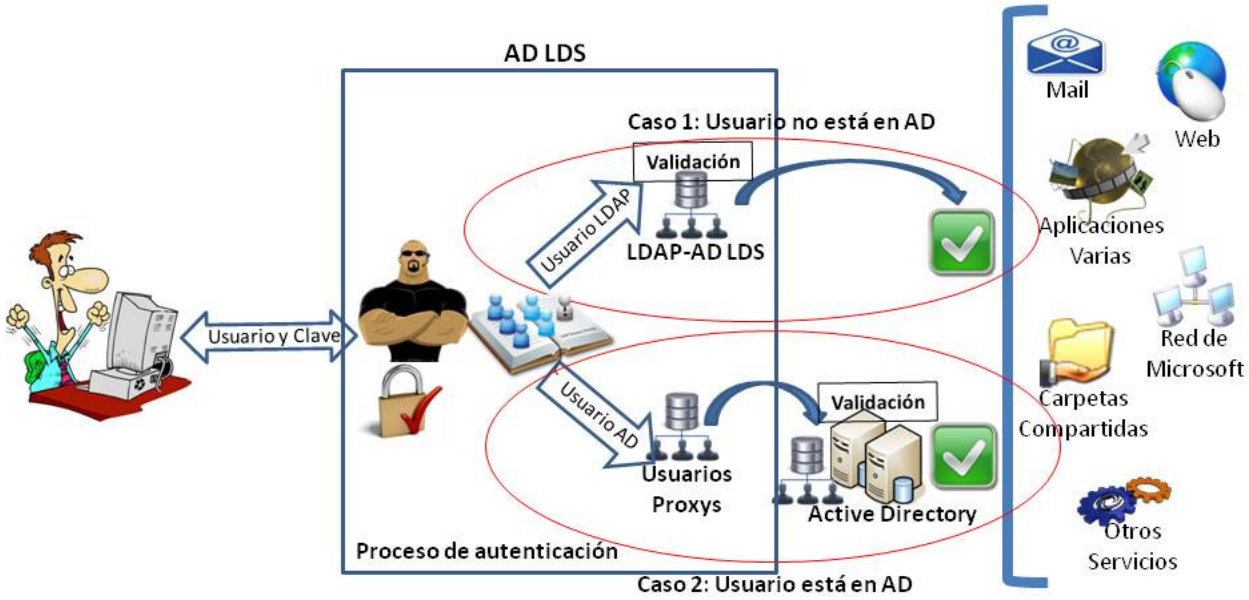


Figura 16: Estructura de la solución propuesta a través de la herramienta AD LDS.

Lo que intenta mostrar la figura anterior, es que el proceso de autenticación del usuario ahora se lleva a cabo contra un solo repositorio el cual se enmarca dentro de un cuadrado de color azul y con el título de "AD LDS". Es decir, que independientemente del servicio/aplicación al que el usuario desee acceder, la autenticación se realizará con credenciales únicas (un único par usuario/clave). Dentro de este proceso de autenticación se siguen teniendo dos repositorios pero de manera totalmente transparente para el usuario que los emplea, dado que en ningún momento notará que su validación impacta contra uno u otro repositorio. Las credenciales del usuario estarán, o bien dentro de Active Directory (sigue siendo ***ADS senasa***), o bien dentro del nuevo LDAP que se muestra, el cual denominaremos de aquí en adelante ***LDAP-AD LDS*** (colocando como sufijo el nombre del nuevo producto AD LDS) sólo con la intención de diferenciarlo del LDAP inicial (***LDAP senasa***), del cual venimos haciendo mención en el documento hasta acá. A simple vista, la solución parece no mostrar muchas diferencias respecto a lo que se tenía hasta ahora. Es decir, dos repositorios distintos y disjuntos. Analizaremos a continuación las distintas componentes que arman esta solución para darle un poco más de luz a la misma.

¿Cuáles son las componentes que forman parte de la solución?

Repositorio de credenciales Active Directory= se trata del mismo servicio de directorio que mencionamos a lo largo de todo el documento, el obtenido como producto de la consolidación de todas las oficinas denominadas como de tipo 1 (***ADS senasa***).

Repositorio de credenciales LDAP-AD LDS= se trata de un repositorio de usuarios con formato LDAP de similares características del que se estuvo haciendo mención hasta ahora con la salvedad que este se implementa con la herramienta de software AD LDS en lugar de ser implementado con el producto OpenLDAP como el anterior. Este repositorio contendrá SÓLO aquellos usuarios que forman parte de ***LDAP senasa***, que no forman parte de ***ADS senasa***. Es decir que entre ***LDAP-AD LDS*** y ***ADS senasa*** no debería haber usuarios en común. Este repositorio difiere de un LDAP común que cuenta con la posibilidad de almacenar un nuevo tipo de usuario denominado usuario proxy que veremos a continuación. En algún momento a lo largo de este documento se mencionó que dentro del servicio ***LDAP senasa*** había unas 6000 cuentas de usuario, y que dentro de ***ADS senasa*** aproximadamente unas 2000. A su vez se mencionó también que estas 2000 cuentas de usuarios ya se encontraban incluidas dentro de las 6000 de ***LDAP senasa***. Es decir, que teníamos una superposición de 2000 cuentas que se encuentran en ambos servicios de directorio. En esta nueva configuración no tendríamos superposición de cuentas, dado que en el ***ADS senasa*** seguiríamos teniendo las 2000 cuentas de usuario, mientras que en el nuevo ***LDAP-AD ADS*** pasaríamos a tener 4000 cuentas. Las cuentas superpuestas pasarían a ser usuarios proxy que veremos a continuación de qué se trata. Tener en cuenta que la diferencia de la cantidad de cuentas a favor de ***LDAP-AD ADS*** se irá decrementando a medida que se vayan incorporando nuevas dependencias de tipo 1 a la infraestructura.

Usuarios proxy= Este es un nuevo concepto que aparece en escena aquí, y que juega un rol muy importante dentro de la configuración de la solución. Los usuarios proxy son como “cáscaras” a la cual se le puede consultar sobre las credenciales de un usuario sin ser un usuario en sí mismo, dado que no almacenan dicha información, sino que cuentan con un puntero que indica dónde debe ser ubicada dicha información. Simplemente para hacer una analogía, se podría decir que son como un acceso directo o puntero a la verdadera posición en donde se encuentra la cuenta de usuario propiamente dicha. Para el caso de la solución aquí planteada, la base de datos de usuarios proxy contiene un indicador hacia Active Directory, donde residirán de manera efectiva las credenciales de los usuarios (nombre de usuario, contraseña, datos personales, oficina, etc). De esta manera, cualquier cambio que sufra el usuario de Active Directory se verá reflejado dentro del proceso de verificación de credenciales, sin necesidad de realizar modificaciones sobre los usuarios proxy, ni sobre el AD LDS.

NOTA: Cabe aclarar que si bien en la figura 16 se ilustran dos bases de datos distintas para los usuarios proxy y para los usuarios LDAP (contenidos en el nuevo ***LDAP-AD LDS***) estos dos tipos de usuario están contenidos en una única base de datos que será la de ***LDAP-AD LDS***, que será sobre la que se llevarán a cabo todas las validaciones de todos los sistemas, aplicaciones, etc. Esto significa que cualquier tipo de autenticación se realiza contra esta base de datos única, y allí es donde se verifica si el usuario a ser validado es de tipo proxy o no. En caso de ser un usuario proxy, el mismo tendrá una referencia al ***ADS senasa*** en donde estarán los verdaderos datos del usuario. En caso contrario, toda la información relacionada al usuario estará almacenada de igual manera a un LDAP común (en este caso estarán en el nuevo LDAP que denominamos ***LDAP-AD LDS***).

Como mencionamos con anterioridad, un usuario proxy no es más que una cáscara que posee una especie de puntero que permitirá obtener la información relacionada al usuario dentro del ***ADS senasa***. Lo descripto se ilustra en la figura 17.

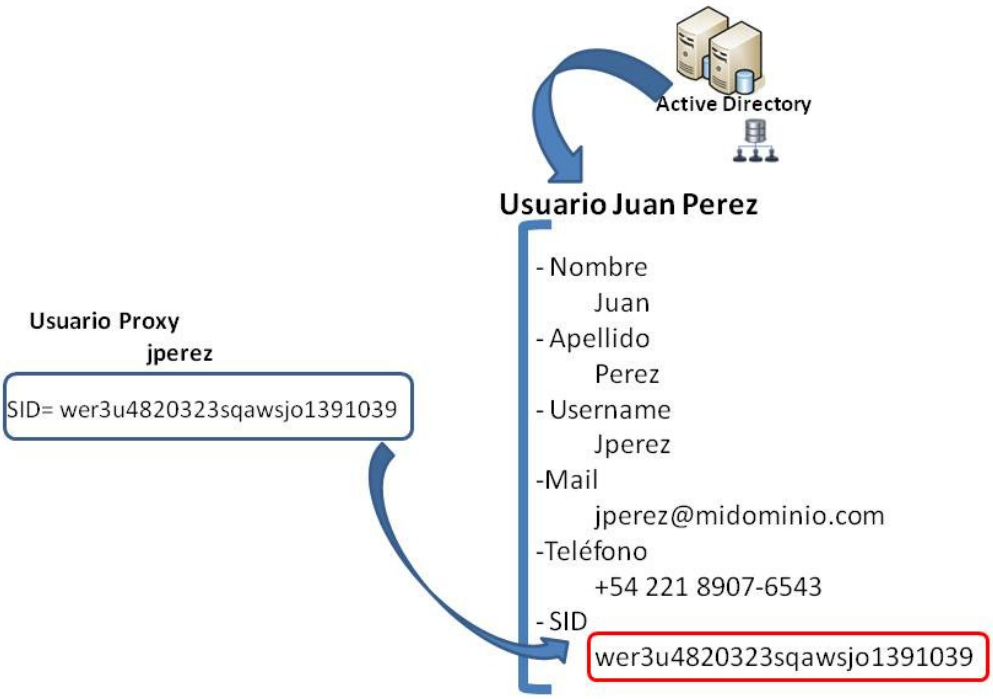


Figura 17: Ejemplo de un usuario proxy

En el caso de la figura 17, el usuario proxy "jperez" y el SID (*Security Identifier* ó *Identificado de Seguridad*) se encuentran almacenados dentro de la base de datos del AD LDS. Será ese SID el que nos permitirá acceder a la información completa de "Juan Perez", información almacenada dentro de la base de datos de Active Directory. Dado que el SID identifica a un usuario de manera unívoca y nunca se modifica a lo largo de la vida útil de un objeto dentro del Active Directory, esta referencia permanecerá activa incluso realizando cualquier tipo de modificación sobre la persona "Juan Perez".

A través de la figura 18 se observa sólo a modo ilustrativo cómo sería la estructura de la base de datos del servicio AD LDS. En la misma pueden observarse tanto usuarios completos (de tipo LDAP) con toda la información asociada a los mismos como ser:

- Username
- Nombre y Apellido
- Clave

como también pueden verse los usuarios de tipo proxy los cuales sólo cuentan con la información que identifica al usuario (SID) dentro de la estructura de ***ADS senasa***.

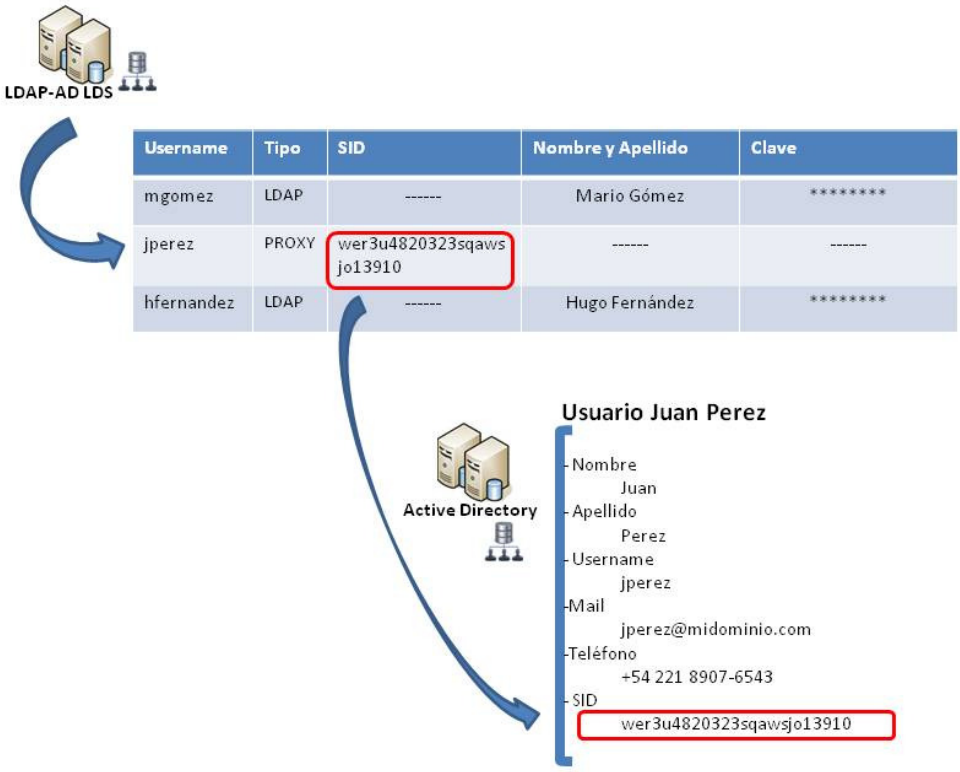


Figura 18: Base de datos de AD LDS

Esta configuración posee todos los beneficios ofrecidos por las herramientas de tipo meta directorio, pero con la diferencia de una mayor simplicidad, y mejor interacción entre las componentes y un costo mucho más reducido en lo que refiere a cuestiones de licenciamiento.

¿Cómo sería el proceso de migración?

Para lograr obtener la configuración deseada, se debe realizar un proceso de migración no menor. El cual consta de comparaciones, validaciones varias y en, o bien volcar los usuarios de ***LDAP senasa*** dentro del nuevo ***LDAP-AD ADS*** o sólo dejar la ocurrencia que ya estaría incluida en ***ADS senasa***. Vemos a continuación una breve descripción de los pasos a seguir para completar la misma:

1- Se debe crear el nuevo ***LDAP-AD LDS*** en base a ***LDAP senasa***. Para ello:
   - Para cada usuario dentro de ***LDAP senasa***,
     - Verificar si también existe dentro de ***ADS senasa***.
       - SI => Sólo dejar la ocurrencia del mismo que existe dentro del ***ADS senasa***. Luego se expondrá sobre los procedimientos realizados para almacenar la clave de la cuenta.

        - NO => entonces el usuario puede ser migrado directamente desde ***LDAP senasa*** al nuevo ***LDAP-AD LDS***.

2- Se debe crear la nueva base de datos de usuarios proxy. Una vez realizado el paso 1, se debe crear para cada usuario dentro de ***ADS senasa***, su correspondiente usuario proxy dentro de la estructura. Esto sería:
    - Para cada usuario dentro de ***ADS senasa***
        - Tomar su SID (identificador único) y crear una objeto proxy (cáscara) dentro del AD-LDS que lo referencie, es decir que almacene dicho SID.

¿Cómo se lleva a cabo el proceso de verificación de credenciales de usuario con esta nueva estructura?

Si bien la solución planteada continúa con la presencia de dos repositorios de usuarios (el ***LDAP-AD LDS*** y ***ADS senasa***) los mismos ya nos son disjuntos, sino que ahora son complementarios y será el AD LDS el responsable de la validación de todas las aplicaciones y servicios que se desee autenticar dentro del Organismo. Obviamente, sólo a excepción del inicio de sesión en red de las terminales de usuario que como no podría ser de otra manera, siempre validarán contra ***ADS senasa***, servicio concebido para tal fin. Entonces, dado que todo impacta sobre AD LDS, y dentro de dicha base de datos tenemos tanto usuarios LDAP comunes, como usuarios proxy, podríamos decir que tenemos ahora dos casos posibles dentro del proceso de verificación de los datos de usuario:

CASO 1= Las credenciales del usuario estaban inicialmente dentro de Active Directory. Es decir, que para este caso, también se tuvo que crear un usuario proxy correspondiente que almacenara el identificador de referencia de dicho usuario dentro de AD LDS. El proceso de verificación se llevará contra la nueva infraestructura (AD LDS) la que verifica la existencia del usuario. Cuando lo encuentra, determina que dicho usuario se trata de un usuario de tipo proxy, y por ende deberá seguir la referencia del mismo para delegar así, el verdadero proceso de verificación de los datos ingresados por el usuario al Active Directory. Por ello la denominación de proxy, que refiere a la estrategia de colocar un “objeto” entre otros dos que realice una especie de pasa manos dentro de un proceso particular. Podemos ver una ilustración a modo de ejemplo en la figura 19.

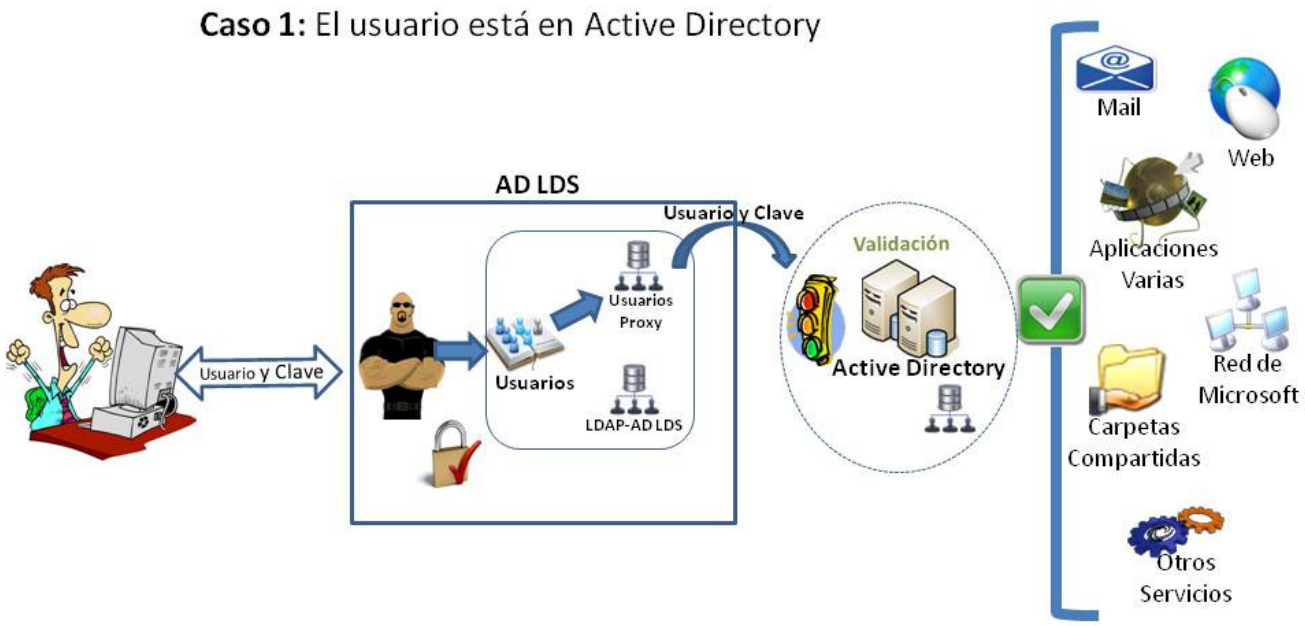


Figura 19: Verificación de datos cuando el usuario está dentro de ADS senasa

CASO 2= El usuario tiene el acceso acotado a una o varias aplicaciones puntuales, pero no tendrá acceso a una terminal de escritorio del Organismo (ya que ese tipo de acceso se lleva a cabo sólo con un usuario de Active Directory). Esto significa que las credenciales de dicho usuario se encontraban en el repositorio que inicialmente llamamos ***LDAP senasa***, (ahora migrado dentro del que llamamos ***LDAP-AD LDS***) y NO en ***ADS senasa***. En este caso, dado que tanto el usuario como la contraseña se encuentran almacenados en el nuevo repositorio, el proceso de verificación de credenciales se llevará a cabo de manera directa sin mayores complicaciones y se ilustra en la figura 20 en donde tenemos el usuario introduciendo las credenciales dentro de la nueva infraestructura de validación.

Figura 20: Verificación de datos cuando el usuario está dentro de LDAP-AD LDS

Beneficios obtenidos

- Políticas de seguridad de usuarios aplicables de manera uniforme tanto para los usuarios de ***ADS senasa*** como los de ***LDAP-AD LDS***.
    - Cambios de clave, fortaleza de clave, expiración, memoria de claves empleadas etc.
- Cada usuario cuenta con una única ocurrencia (en alguno de los dos repositorios)
- Única clave para cada persona.
- Replicación multi master.
- Fácil implementación de la tolerancia a fallas (por la replicación)
- Permite una fácil modificación del esquema de los usuarios en caso de ser necesario modificar la información necesaria para los usuarios. Por ejemplo agregar el dato DNI para cada uno de los usuarios.
- Solución probada y confiable.

Problemas planteados y decisiones tomadas

1. Los usuarios que se encontraban tanto en ***ADS senasa*** como en ***LDAP senasa*** podrían tener dos claves distintas en cada uno de los repositorios. ¿Cómo unificarlas teniendo en cuenta que dichas claves están cifradas en ambos repositorios?

El primer problema que surge a la hora de querer realizar la unificación de credenciales es que tanto en LDAP como en Active Directory las claves de los usuarios allí almacenados se encuentras cifradas, y por ende ilegibles incluso para el usuario de mayor nivel de acceso sobre la estructura. Esto significa que no es posible tomar un usuario de un repositorio y simplemente copiarlo en el otro ya que no tendremos el efecto esperado sobre las claves. Esto genera la necesidad que todos los usuarios deban actualizar algunos de sus datos para compatibilizarlos a la nueva estructura.

2. ¿Qué sucede en caso que sea necesario mover un usuario de un repositorio a otro luego de la migración?

   A. Un usuario que se encontraba almacenado dentro de ***ADS senasa*** debe ser "movido" al ***LDAP-AD ADS***. Esto podría suceder en el supuesto caso en que se recortaran las funciones de dicha persona dentro del Organismo. En este caso los pasos a seguir serían crear el usuario dentro del ***LDAP-AD LDS*** con los datos que correspondan, y eliminar la correspondiente en ***ADS senasa***. De todos modos este caso sería excepcional, dado que una vez que el usuario ha sido creado dentro de ***ADS senasa***, no existe motivo para no mantenerlo dentro de dicho repositorio y hacer que las validaciones se realicen allí.

   B. Por el contrario un usuario almacenado en ***LDAP-AD ADS*** requiere permisos para iniciar sesión en las terminales de manera interactiva empleando los servicios de Active Directory. Esto significaría "mover" dicho usuario desde ***LDAP-AD LDS*** hacia ***ADS senasa***. En este caso, lo que habría que hacer es crear el usuario en ***ADS senasa***, crear el usuario proxy correspondiente dentro de AD ADS, y por último eliminar el usuario que deja de cumplir funciones que se encontraba en el repositorio ***LDAP-AD LDS***.

3. ¿Cómo distribuir los servidores geográficamente en el país con el AD LDS?

   Este punto es neurálgico para la solución, lo que significa que debe ser muy tenido en cuenta. Se trata de pensar dónde se colocarán los servidores físicos que contendrán una réplica de la base de datos de usuario con el AD LDS. Teniendo en cuenta la complejidad de la red del Organismo que hemos analizado, las opciones son muchas (la combinación de posibilidades con las oficinas de acuerdo a su importancia).

   Es oportuno recordar en este momento que al momento de realizar la implementación de ***ADS senasa*** en todas las dependencias de tipo 1, se concluyó que lo mejor era contar con dos equipos físicos en cada una de las dependencias. Esto evitaría las interrupciones de servicio en caso de caída de uno de los servidores (dado que el otro seguiría funcionando) y a su vez, en caso de caída del enlace con Casa Central, si bien podríamos dejar de tener acceso a la base de usuarios de las aplicaciones corporativas (en ese momento ***LDAP senasa***), tampoco tendríamos acceso a las aplicaciones en sí, dado que estas también residen en Casa Central. Esto se ilustró oportunamente a través de la figura 11.

   Recordemos también, que al momento de evaluar las ventajas de esta solución, se mencionó sobre la facilidad que la misma ofrece al momento de llevar a cabo la replicación de las distintas ocurrencias de bases de datos que haya distribuidas. Dicha replicación se realiza de manera similar a la que efectúa la solución Active Directory, es decir de manera multi

master. Esto significa que los cambios pueden ser realizados en cualquier servidor que forme parte de la estructura de validación, y dicho cambio se replicaría hacia el resto de una forma natural y transparente para los administradores de infraestructura. Entonces al momento de evaluar la distribución de servidores geográficamente si bien las opciones son varias, nos quedaremos sólo con un par que son:

A. Uno o más servidores *SÓLO* en Senasa Central contienen la base de datos del AD LDS. De esta manera todos los cambios se llevarían a cabo en alguno de estos equipos, y luego se replicarían al resto. La figura 21 muestra de manera gráfica lo expuesto.

Ventajas:

- Simplicidad dada a la menor cantidad de réplicas de la base de datos(mantenimiento, configuración)
- Seguridad, teniendo en cuenta que la base de datos no se encuentra diseminada en cada una de las dependencias.

Desventajas

- Si se cae el enlace con Senasa Central, desde las dependencias no se tendría acceso a la base de datos del AD LDS (NOTA: Si a ***ADS senasa***, dado que hay que recordar que la misma tiene instancias en todas las dependencias de tipo1). Aunque si bien no se tendría acceso al AD LDS, como se comentara en párrafos anteriores, tampoco se tendría acceso a las aplicaciones corporativas que son accedidas vía la validación del directorio en cuestión. Esto es porque dichas aplicaciones prestan servicio sólo desde *Senasa Central*.

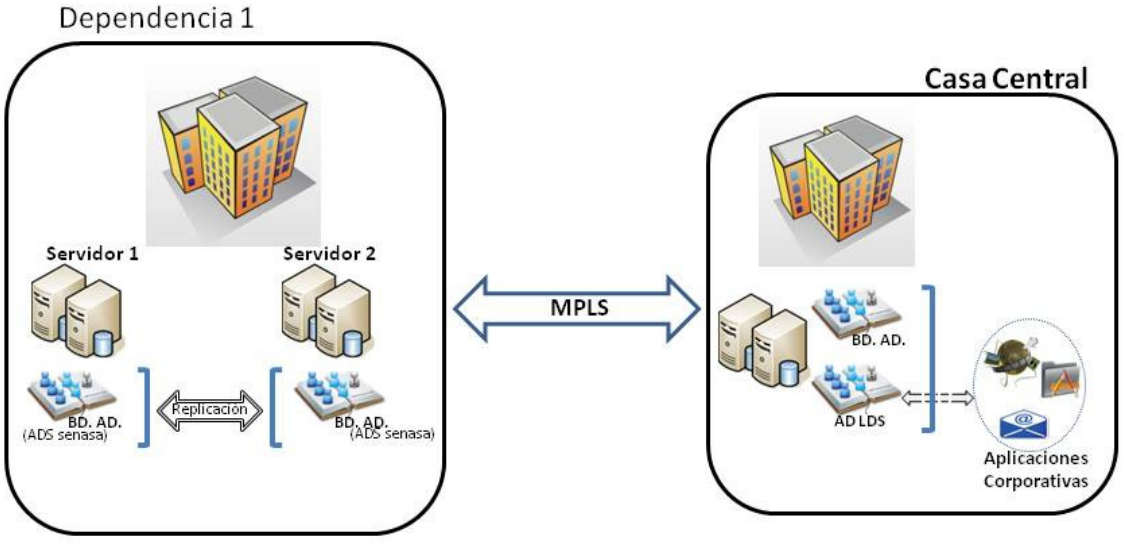


Figura 21: La base de datos del AD LDS sólo en Casa Central

B. Al menos un servidor en cada oficina de tipo 1 contendrá una réplica de la base de datos del AD LDS. Esta estructura de servidores sería similar a la distribución de servidores de tipo controlador de dominio[29] que se realizó para la implementación de Active Directory en todas las oficinas de tipo 1 en todo el país. Recordemos que para ello se colocaron dos equipos físicos en cada oficina de tipo 1 de manera de contar con redundancia dentro de cada oficina, y a la vez no ver interrumpido los servicios en caso de caída del enlace de red que vincula la oficina con *Senasa Central*. La disposición para cada oficina de tipo 1, se ilustra a través de la figura 22.

Ventajas

- Permite mantener acceso a los datos del AD LDS en caso de caída de vínculo contra Senasa Central. Aunque aún con acceso a dicha base de datos, quizás no tengamos acceso a las aplicaciones corporativas.

Desventajas

- Más complejo

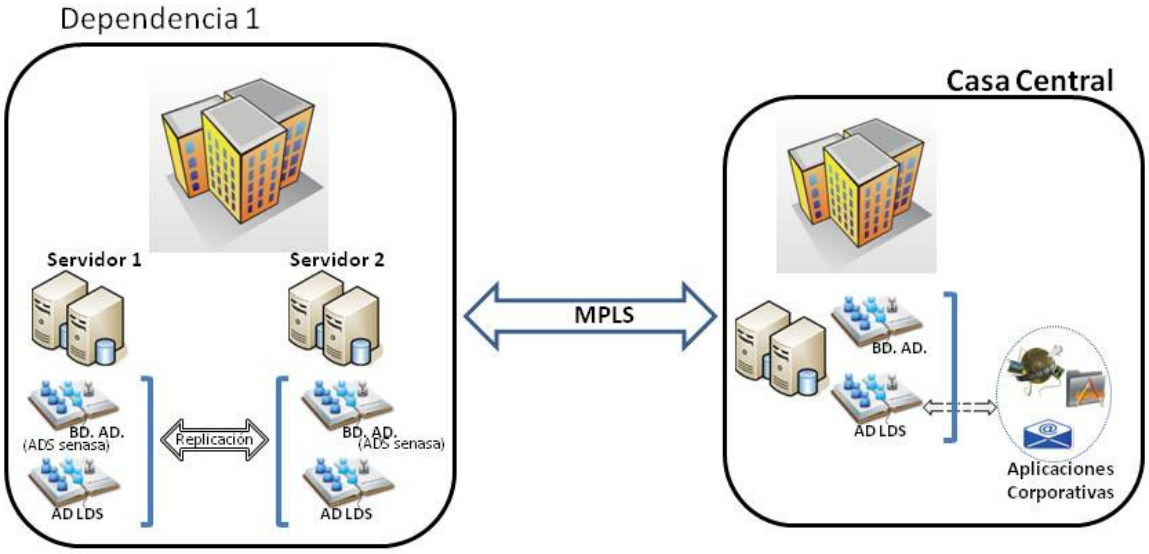


Figura 22: La base de datos del AD LDS en cada dependencia de tipo 1

En base a lo expuesto en las alternativas, la respuesta a la mejor manera de distribuir los servidores del servicio AD LDS dentro de la estructura de servicios de Senasa, es la expresada a través del punto A, es decir "Uno o más servidores SÓLO en Senasa Central contienen la base

[29] *Ver **Glosario** al final del documento*

de datos de AD LDS". Esta decisión se basa más que nada en la sencilla razón que las aplicaciones y servicios corporativos, también se encuentran sólo en *Senasa Central*, por lo cual una eventual interrupción del enlace de red entre una oficina y Senasa Central impediría no sólo el acceso a los servidores con la base de datos del AD LDS; sino también impediría el acceso a dichos servicios/aplicaciones. Por tal razón no se justifica tener réplicas con los datos del AD LDS dentro de las dependencias de tipo 1.

Adicionales

A la hora de llevar a cabo este gran cambio, surgió la presencia de un gran número de aplicaciones y servicios que debían modificar su proceso de validación de usuarios. Es decir, aplicaciones que validaban contra ***LDAP senasa***, y que ahora deberían ser re configuradas para realizar el mismo proceso contra el nuevo AD LDS. Este cambio llevó un gran tiempo hasta poder determinar la totalidad de dichas aplicaciones, y llevó a tomar la decisión de implementar una nueva "capa" dentro de este proceso de validación de usuarios que realizan las aplicaciones. Una capa de abstracción entre las aplicaciones y el repositorio de usuarios contra el cual las mismas validan. De esta manera, esta capa sería la encargada de determinar cuál es el repositorio contra el cual se conectará, y abstraerá a las aplicaciones del mismo. Es decir, que en otro futuro cambio, el impacto sería absorbido por esa capa y no sería necesario volver a modificar cada una de las aplicaciones en cuestión.

Todas las aplicaciones y servicios del Organismo se conectaban directamente contra el repositorio de usuarios LDAP realizando consultas directamente contra su BD. Esto se puede observar a través de la figura 23 en donde se ilustra dicha conexión directa. De esta manera cualquier modificación en el proceso de validación de usuarios como por ejemplo en el equipo servidor, ó forma de almacenamiento de claves, requerirá modificar los parámetros de conexión en cada una de las aplicaciones y servicios que lo emplean.

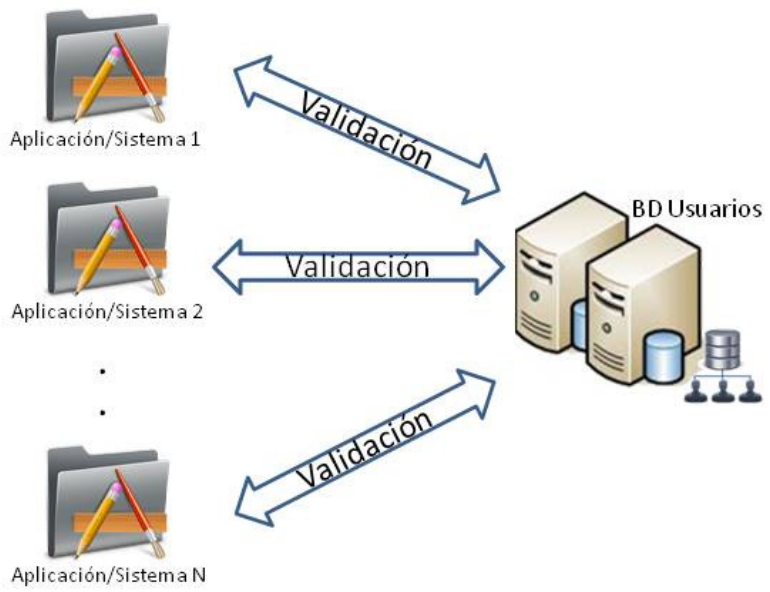


Figura 23: Las aplicaciones se conectan de manera directa a la base de datos de usuarios

Los cambios llevados a cabo en el proceso de validación mediante la introducción del AD LDS requirieron la modificación de los parámetros de conexión al repositorio de validación en todos los servicios y aplicaciones existentes en el Organismo. Por tal motivo se tomó la decisión de aprovechar dicha situación para aplicar una mejora sustancial dentro de la configuración de los servicios/aplicaciones antes citados, incorporando una nueva capa de abstracción. Dicha capa sólo se encarga de contener los parámetros específicos de conexión hacia el repositorio de usuarios. Entonces, las aplicaciones y servicios apuntarían a dicha capa, y sólo allí se encontrarían los valores específicos tales como:

- Nombre del servidor
- Puertos
- Protocolos
- Nombres de usuario y contraseñas para realizar la conexión (en caso de ser necesario)
- Consultas necesarias para obtener la información necesaria para lograr la conexión
- Etc.

Desde el punto de vista de la estructura de la solución, podemos ilustrar a través de la figura 24 cómo se ordenaría cada una de las componentes que forman parte en la misma.

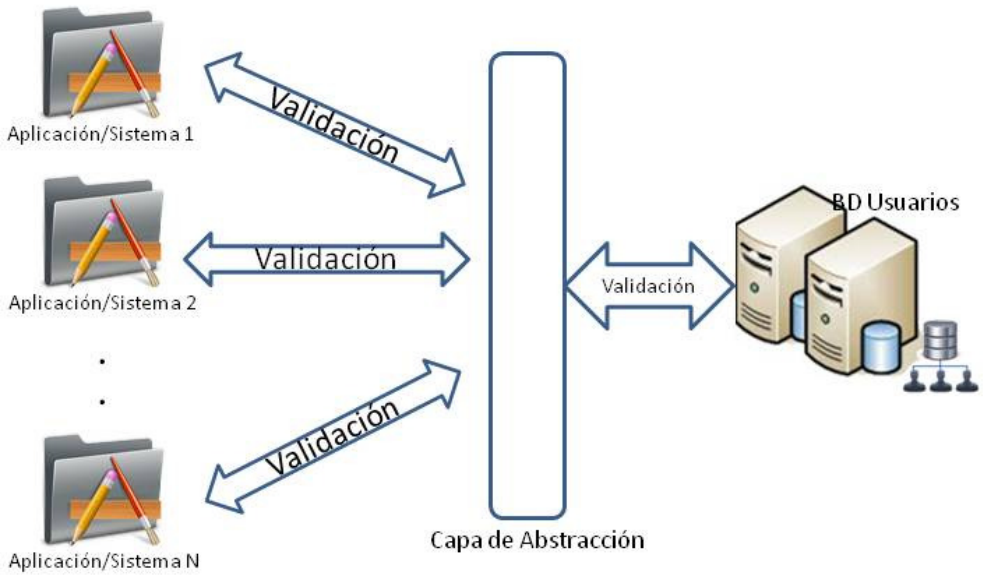


Figura 24: Capa de abstracción entre las aplicaciones y la base de datos de usuarios

6. Beneficios obtenidos

Los beneficios obtenidos a partir de esta nueva implementación, ya han sido tratados a lo largo de todo el documento, pero teniendo en cuenta que los mismos son muchos y de gran magnitud, considero oportuno volver a describirlos en esta sección donde se listarán y detallarán. Dichos beneficios justifican por sí solos todos los trastornos que pudieran ocasionar los procesos de la implementación, los cuales han sido muchos, pero en su mayoría no de ”graves” si consideramos como graves, aquellos cambios que tienen alto impacto sobre el labor diario del usuario final. Esto claro, teniendo en cuenta que nos referimos a un Organismo con más de 6000 personas trabajando diariamente en donde cualquier cambio de relevancia, podría llegar a producir un efecto negativo hacia el cambio, aún cuando el mismo introduzca innumerables beneficios desde todo punto de vista. Por ello, se debe ser muy cuidadoso al momento de realizar las modificaciones.

A modo de recordatorio y de manera de poder hacer más énfasis en el detalle de algunos de los beneficios que se introdujeron a partir de la implementación, haremos un muy breve repaso de cómo se determinó que sería la infraestructura de servicios en cuanto a la distribución de los mismos dentro del mapa de las dependencias de Senasa.

Casa Central:

- Dos o más servidores controladores de dominio para dar sustento a ***ADS senasa***.

- Dos o más equipos con la base de datos del AD LDS, pudiendo incluso hasta ser los mismos servidores físicos donde se ejecutan los roles de controladores de dominio (no recomendado).

Dependencias de tipo 1:

- Dos o más servidores controladores de dominio para dar sustento a ***ADS senasa***.
- No se dará sustento a la base de datos del AD LDS dado que la misma sólo estaría en Casa Central, teniendo en cuenta que es allí donde están las aplicaciones corporativas.

Con esta estructura, analicemos entonces los beneficios logrados tipificados según diversos aspectos.

6.1 Desde el punto de vista de la administración

Sin intención de confeccionar un manual de Active Directory, ni de las bondades que este ofrece a cualquier gran entorno corporativo de TI, se dirá que los beneficios desde el punto de vista de la administración han sido notables y han logrado facilitar en gran magnitud las tareas rutinarias que se realizaban sobre la infraestructura informática del Organismo.

- Movilidad de usuarios: Los usuarios se definen en un solo lugar y allí se le otorgan los permisos para acceder a los recursos de la oficina que corresponda. Es decir que con el mismo usuario, podrá hacer uso de cualquier recurso de información que forme parte de la infraestructura.
- Directivas de Seguridad centralizadas: Se pueden definir de manera centralizada, políticas que permitan establecer parámetros de configuración para usuarios y PCs dentro de todo el país. Esto abre un gran abanico de opciones, entre las que podemos citar las siguientes sólo para mencionar algunas:
    - Instalación remota de software
    - Definición de restricciones sobre la terminal de trabajo
- Administración de PCs/servidores: Todos los equipos ahora son accesibles con usuarios pertenecientes a un único repositorio de usuarios. Es decir, que otorgando los privilegios correspondientes a ese único usuario se podría tener acceso a cualquier equipo de la red. Sin duda esto abre también una gran puerta de inseguridad, pero si se emplea con los debidos cuidados y responsabilidades, se trata de una posibilidad inmejorable para facilitar la tarea diaria relacionada a la administración de un número tan elevado de equipos, con un grupo reducido de personas.
- Atención a usuarios: Este es un punto también relevante, dado que ahora uno puede tener más noción de los verdaderos problemas de los usuarios al conocer más y mejor

sobre la estructura sobre la que trabajan dado que la misma se acota en gran medida. A su vez, de manera centralizada uno como administrador cuenta con más y mejores herramientas de hardware y software tanto para monitorear los recursos, como para establecer parámetros de normalidad dentro del funcionamiento integral de la infraestructura.

- Conocimiento de los recursos del organismo: Este punto quizás parezca de no tanta importancia, pero al momento de realizar la implementación se logró tener certeza de información realmente relevante como cantidad y ubicación de PCs, usuarios, aplicaciones instaladas, etc. Información que todos el tiempo se desea tener y con la mayor precisión posible para contar con un relevamiento en todo momento de la Organización y del consumo de recursos de TI.
- Escalabilidad: A partir de los cambios analizados en el presente trabajo, se simplifica de manera notable la incorporación de nuevos servicios. Esto está motivado no sólo por la unificación de los repositorios de usuarios, sino también por el trabajo adicional que se explicara en secciones anteriores al colocar una capa de abstracción entre las aplicaciones y las bases de datos donde residen las credenciales de usuarios (Figura 24).

6.2 Desde el punto de vista de la seguridad

Sin duda este punto es otro de los puntos fundamentales en los que la solución propuesta se hace fuerte. Esto teniendo en cuenta que se tuvieron en cuenta varias cosas como para no dejar al azar aspectos relacionados al tema de la seguridad.

- Acceso a servicios y aplicaciones: Se cuenta con una granularidad mucho más fina para llevar a cabo el control del acceso a los servicios y a las aplicaciones existentes. A su vez, esto tiene que ver con la información que se tiene acerca de, por ejemplo, las actividades que realiza un determinado usuario de la red, y desde qué ubicación geográfica. Información que antes no se podía obtener.
- Derechos de usuarios: Se logra administrar de manera mucho más sencilla lo que tiene que ver con los derechos de los usuarios, no sólo para acceder a los recursos de la organización, sino también para algo que siempre se tornó complejo como es el manejo de los roles dentro de las aplicaciones. A partir de ahora, y con la centralización del manejo de las credenciales de usuario, podremos estar seguros que los permisos que posee la única cuenta, totaliza todos los derechos que el usuario tendrá sobre los mencionados recursos. Es decir, que no habrá otro usuario distinto dentro de otro repositorio distinto que pudiera otorgarle o quitarle derechos a los contenidos en el repositorio centralizado.
- ABMs: sin duda un proceso engorroso dentro de los procedimientos dentro de una organización es el de las altas, bajas y modificaciones de usuarios con la asociación correspondiente de permisos/derechos sobre los recursos. A partir de aquí, este

proceso se llevará a cabo una única vez, en un solo repositorio y podremos tener la certeza que una baja aquí, inhabilita el acceso de ese usuario a cualquier recurso ubicado en cualquier punto del país.

- Concientización de las personas sobre la importancia de SU usuario: A partir de esta nueva implementación, las personas toman conciencia de la importancia que tienen sus credenciales de usuario, que son nada más y nada menos que su identificación dentro de los recursos del Organismo, las llaves para poder acceder a los datos. Con configuraciones anteriores, era normal que alguien "prestara" sus credenciales de usuario para poder ingresar a una PC, para poder navegar por internet. Ahora, al contar con una única, lo pensará dos veces.
- Continuidad del servicio: Dado que se introdujeron un gran número de servidores dentro de la topología del Organismo a nivel nacional, y teniendo en cuenta cómo los mismos replican entre sí toda la información crítica relacionada a los usuarios, se incorpora un eslabón fuerte dentro de la cadena para intentar mitigar posibles interrupciones de servicio. Esto tiene que ver con que no todas las bases de datos importantes se encuentran sólo en Casa Central, lo que significa que algunas aplicaciones podrían seguir operando aún en caso de caída de vínculos de red.

6.3 Desde el punto de vista de la visión unificada de la organización

Finalmente y a partir de esta implementación, se puede afirmar que se cuenta con visión unificada de la organización al menos en lo que refiere a infraestructura de TI. Podemos visualizar dentro del mapa de la República Argentina, y ver las distintas dependencias de tipo 1, como piezas de un complejo rompecabezas, piezas de un todo, y no partes independientes con limitada interacción como se describiera al inicio de este estudio.

- Visión general de las dependencias de tipo 1: A partir de ahora, teniendo en cuenta que todas las dependencias cuentan con una configuración similar, la visión de las mismas es genérica. Los problemas que le pudieran suceder a una, se repiten en las demás así como en general también las soluciones. Por el contrario, antes cada dependencia era un mundo independiente, con sus propios problemas casi únicos, dado que cada dependencia contaba con un enorme conjunto de particularidades lo cual agregaba un condimento más a la complejidad del problema.
- Foros de referentes: Teniendo en cuenta el punto anterior, se logró formalizar un grupo de referentes en tecnología, los cuales pueden compartir experiencias, conocimientos, plantear dudas o lo que fuere.

6.4 ¿Qué sucede con las dependencias de tipo 2?

Hasta aquí mucho se dijo de las modificaciones incorporadas y de los muchos beneficios que los mismos introdujeron a la Organización. Pero también se mencionó que dichos beneficios eran sólo para las dependencias de tipo 1, es decir aquellas que cumplen con la condición de poseer un vínculo de red de tipo dedicado con Casa Central entre otras.

A su vez, también se mencionó en las primeras secciones de este documento (para ser más precisos en la sección 4.2.2, al momento de describir la infraestructura de servicios con la que se trabajaría) que se asumía como generalidad en el tipo oficina del Organismos a las de tipo 1, teniendo en cuenta que se contaba con la decisión de dotar a las dependencias de tipo 2, de la tecnología y de la infraestructura en general para convertirlas en dependencias de tipo 1. Esto nos permitió pensar en una solución más integral y unificada al momento de evaluar las condiciones para la implementación.

Por lo antes mencionado es que poco se dijo de las dependencias de tipo 2 que al momento de iniciado el presente trabajo entre Oficinas Locales, puertos, pasos de frontera y demás dependencias que encuadran en este tipo, podemos contabilizar aproximadamente 500 (quinientas) oficinas.

Las razones por las cuales no se consideraran estas dependencias (al menos no hasta que no cuenten con las características deseables mínimas para almacenar equipos e información crítica) tienen que ver con aspectos de infraestructura esenciales para cualquier implementación que no son cubiertos por las mismas. Aspectos obvios que quizás hayan quedado en manifiesto a lo largo del documento, pero que de todos modos describiremos sin entrar en detalles. Muchos de estos tienen que ver con una infraestructura de oficina más humilde, en la que trabajan y se atienden a menor cantidad de personas respecto a las oficinas descriptas como dependencias de tipo 1. Algunos de estos aspectos son:

- Ausencia de seguridad física: Para realizar la nueva implementación, cada dependencia fue provista de al menos dos servidores, switchs, UPSs, firewall y sin tener en cuenta la relevancia de la información que luego se replicaría en los servidores. Información relacionada a las bases de datos de los usuarios de todo un Organismo. Sin duda este aspecto es determinante para la implementación, teniendo en cuenta la relevancia de los recursos que se ponen en juego.
- Infraestructura edilicia: Aspectos tales como la necesidad de contar con una sala de servidores dotada de aire acondicionado, rack, suministro confiables de energía eléctrica (detalle no siempre previsible en localidades del interior del país)
- Ausencia de enlaces de red confiables: este punto también es determinante a la hora de tomar la decisión de incorporar una nueva oficina a la nueva infraestructura de replicación. Esto es así, dado que dicho enlace será en encargado de mantener los datos no sólo actualizados, sino también consistentes. Y en caso que el mismo no

fuera confiable en cuanto a estabilidad, seguridad, esta tarea sería por demás complicada, e incorporaría problemas en toda la topología de replicación.

7. Conclusiones

7.1 Aspectos destacados

Las modificaciones sugeridas en el presente documento, si bien introducen un gran cambio a nivel infraestructura de hardware requerida, con la complejidad adicional que esto insume, introducen también una gran cantidad de beneficios desde diversos puntos de vista. Algunos de ellos tienen que ver con la administración de los recursos informáticos, facilidad para incorporar futuras implementaciones (sistemas, extensiones departamentales, recursos compartidos, etc) de manera más natural y sencilla. Pero desde la visión del usuario final, estamos incorporando el valor agregado fundamental de contar con único par Usuario/Clave para TODOS los recursos de información a los que tenga acceso. Este punto en el mundo TI de hoy en el que conviven un gran número de fuentes de información, muchos de los cuales se heredan de muchos años atrás es sin duda un logro para no despreciar. Más aún teniendo en cuenta el tipo de Organismo sobre el cual se llevó a cabo el trabajo, un Organismo de gran envergadura y con una dispersión geográfica con pocas entidades que se comparen en toda la Argentina.

Sumado a que las credenciales serán únicas, las mismas estarán centralizadas en un "único" repositorio con todos los beneficios que dicha estructura acarrea a nivel administrativo.

Además de ello, y de acuerdo a como se describió en el presente documento, la posibilidad de implementar directivas de seguridad de manera centralizada las cuales se replicarían en forma de cascada a lo largo de todos los equipos (estaciones de trabajo y/ó servidores) sin necesidad de repetir las mismas tareas rutinarias en varios equipos.

Como experiencia profesional, sin dudarlo ni un minuto cierro los ojos y haciendo un recuento de las tareas realizadas para llegar al punto en donde nos encontramos hoy como Organización, tengo que decir que me encuentro más que satisfecho por la oportunidad no sólo de haber podido planear, imaginar, diseñar una solución, sino también de poder llevarla a cabo y hoy poder ver los resultados obtenidos. Obviamente que nada de lo hasta aquí expuesto es obra exclusivamente mía, sino de un gran equipo de personas que remaron en todo momento hacia el mismo lado, con la misma idea de mejorar una estructura de TI.

7.2 Situación a la fecha

Al día de hoy y en lo que refiere a la problemática planteada bajo el título de "Visión disgregada del Organismo" la implementación descripta a lo largo del presente trabajo, si bien se encuentra en un estado avanzado aún no puede darse como finalizada. Cabe destacar que dicha problemática decidió atacarse mediante la implementación de un único Active Directory para todo el país. En este sentido, los primeros resultados son por demás satisfactorios teniendo en cuenta los grandes beneficios obtenidos muchos ya descriptos a lo largo del presente documento. Esto ha llevado a seguir con el mismo rumbo no sólo hacia todas las dependencias de tipo 1 que hoy existen dentro del Organismo, sino también a expandir la infraestructura hacia las futuras dependencias tipo 1 que habrá. Sin duda será un gran esfuerzo, pero a la vista ya se pueden observar grandes resultados.

A la fecha, se puede decir que la implementación se ha realizado de manera exitosa en:

- La totalidad de Casa Central
- 14 (catorce) Centros Regionales
- 2 (dos) Laboratorios
- En vías de incorporar las 12 (doce) oficinas principales. Previsto para el transcurso del año 2013.

En cuanto a la segunda problemática planteada en el presente trabajo, y tratada bajo el título de "Dos grandes repositorios disjuntos" y en lo que refiere a la situación actual, la implementación se encuentra en una etapa final a la espera de ser pasada al estado de producción. Se llevaron a cabo algunas de las tareas más complejas como ser el filtrado y migración de datos, configuración de las aplicaciones a través de la capa de abstracción incorporada y analizada bajo el título "Adicionales" de la sección 5.2.2. Se configuraron varios servicios dentro de un entorno de prueba bajo esta nueva modalidad. Se espera que para el mes de Mayo de 2013 todas las aplicaciones y servicios del Organismo funcionen bajo esta nueva modalidad.

7.3 ¿Dónde es aplicable esta solución?

Si bien toda la descripción que se ha brindado a través del presente documento, se realizó teniendo como referencia al Organismo Senasa, se puede afirmar que no es sólo aplicable para este Organismo y que este caso, podría replicarse en otros casos similares.

Sin ir más lejos, me ha tocado participar en reuniones de intercambio técnico entre organizaciones del Estado, en las que surgen problemáticas como la aquí planteada, y se debaten soluciones aplicables. En este sentido, y gracias a la cercanía que Senasa posee con el INTA

(Instituto Nacional de Tecnología Agropecuaria [31]) y no sólo desde el punto de vista de la distancia, sino también teniendo en cuenta que ambos organismos son los dos grandes ejes que conforman el Ministerio de Agricultura, Ganadería y Pesca de la Nación además de compartir aspectos tales como:

- Desarrollo e infraestructura tecnológica
- Distribución y dispersión geográfica de los recursos informáticos
- Gran número de sistemas de información
- Varios repositorios de usuarios
- Red de PCs con sistema operativo de la familia Microsoft

Se llega a la conclusión que para el INTA la solución que se ha desarrollado a lo largo de este documento, no sólo es aplicable también, sino que gracias a la cordial relación entre los dos Organismos, el INTA está en vías de adoptar la misma. Situación que de alguna manera me hace pensar que el esfuerzo ha valido la pena.

7.4 A futuro

Por suerte la historia no termina aquí, dado que a un hito le sucede otro y las demandas de evolución con respecto a la tecnología no cesan. Esto convierte en un desafío constante esta profesión, no sólo desde el punto de vista técnico, sino también en el reto personal de no poder darse el lujo de desactualizarse, sino por el contrario de deber mantenerse "al día" con las novedades que surgen y que pudieran llegar a simplificar nuestra tarea diaria.

En este sentido, se esperan aún grandes innovaciones desde el punto de vista tecnológico en Senasa, innovaciones muchas de las cuales quizás no tenga sentido mencionar en este trabajo de investigación pero si hay una particularmente importante que adopta una particular importancia luego de haber llevado a cabo la implementación replicada de directorios de usuario que se ha descripto aquí. Se trata de la expansión de la red "***red unificada de servicios***". Nos referimos a que se han iniciado las gestiones para que la gran mayoría de dependencias de tipo 2, se conviertan en oficinas de tipo 1 con todo lo que ello implica para el próximo año. Se trata de más de 440 (cuatrocientas cuarenta) oficinas que se estima contarían con un vínculo dedicado con Casa Central en el futuro. Esto sin duda, es el puntapié inicial para iniciar un gran número de actividades tendientes a seguir extendiendo esta nueva infraestructura para seguir cubriendo puntos estratégicos dentro de la red de dependencias del Organismo. Sin dejar de lado obviamente, los detalles relacionados a seguridad, infraestructura edilicia y otros puntos de vital importancia que cualquier oficina deberá cumplir sin excepción para ser parte activa de esta gran red distribuida de información, detalles a tratar con el tiempo dado que muchos de los mismos requieren de grandes inversiones económicas para abastecer de recursos mínimamente de hardware y software.

Anexos

Anexo I: Active Directory Services (ADS)

Active Directory (AD) es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos (principalmente LDAP, DNS, DHCP [32], Kerberos [33]).

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.

Active Directory permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera. Active Directory 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.

Estructura

Active Directory está basado en una serie de estándares llamados X.500, aquí se encuentra una definición lógica a modo jerárquico.

Dominios y subdominios se identifican utilizando la misma notación de las zonas DNS, razón por la cual Active Directory requiere uno o más servidores DNS que permitan el direccionamiento de los elementos pertenecientes a la red, como por ejemplo el listado de equipos conectados; y los componentes lógicos de la red, como el listado de usuarios.

Un ejemplo de la estructura descendente (o herencia), es que si un usuario pertenece a un dominio, será reconocido en todo el árbol generado a partir de ese dominio, sin necesidad de pertenecer a cada uno de los subdominios.

A su vez, los árboles pueden integrarse en un espacio común denominado bosque (que por lo tanto no comparten el mismo nombre de zona DNS entre ellos) y establecer una relación de o confianza entre ellos. De este modo los usuarios y recursos de los distintos árboles serán visibles entre ellos, manteniendo cada estructura de árbol el propio Active Directory.

Objetos

Active Directory se basa en una estructura jerárquica de objetos. Los objetos se enmarcan en tres grandes categorías:

- Recursos (impresoras)
- Servicios (correo electrónico)
- Usuarios (cuentas de usuario y grupos)

El AD proporciona información sobre los objetos, los organiza, controla el acceso y establece la seguridad.

Cada objeto representa una entidad individual — ya sea un usuario, un equipo, una impresora, una aplicación o una fuente compartida de datos— y sus atributos. Los objetos pueden contener otros objetos. Un objeto está unívocamente identificado por su nombre y tiene un conjunto de atributos (las características e información que el objeto puede contener) definidos por y dependientes del tipo. Los atributos, la estructura básica del objeto, se definen por un esquema, que también determina la clase de objetos que se pueden almacenar en el AD.

Funcionamiento

Su funcionamiento es similar a otras estructuras de LDAP (Lightweight Directory Access Protocol), ya que este protocolo viene implementado de forma similar a una base de datos, la cual almacena en forma centralizada toda la información relativa a un dominio de autenticación. La ventaja que presenta esto es la sincronización presente entre los distintos servidores de autenticación de todo el dominio.

A su vez, cada uno de estos objetos tendrá atributos que permiten identificarlos en modo unívoco (por ejemplo, los usuarios tendrán campo «nombre», campo «email», etc, las impresoras de red tendrán campo «nombre», campo «fabricante», campo «modelo», campo "usuarios que pueden acceder", etc). Toda esta información queda almacenada en Active Directory replicándose de forma automática entre todos los servidores que controlan el acceso al dominio.

De esta forma, es posible crear recursos (como carpetas compartidas, impresoras de red, etc) y conceder acceso a estos recursos a usuarios, con la ventaja que estando todos estos objetos memorizados en Active Directory, y siendo esta lista de objetos replicada a todo el dominio de administración, los eventuales cambios serán visibles en todo el ámbito. Para decirlo en otras palabras, Active Directory es una implementación de servicio de directorio centralizado en una red distribuida que facilita el control, la administración y la consulta de todos los elementos lógicos de una red (como pueden ser usuarios, equipos y recursos).

Anexo II: Active Directory Lightweight Directory Service (AD LDS)

Es un servicio de directorio (LDAP), que proporciona almacenamiento y recuperación de datos a aplicaciones habilitadas para el uso de directorios, sin las dependencias necesarias para los Servicios de dominio de Active Directory (AD DS).

¿Qué hace AD LDS?

AD LDS proporciona una compatibilidad flexible para las aplicaciones habilitadas para el uso de directorios. Una aplicación habilitada para el uso de directorios usa un directorio (en lugar de una base de datos, un archivo sin formato u otra estructura de almacenamiento de datos) para guardar sus datos. Los servicios de directorio (como AD LDS) y las bases de datos relacionales proporcionan mecanismos de almacenamiento y recuperación de datos, pero están optimizados de formas diferentes. Los servicios de directorio están optimizados para el procesamiento de lecturas, mientras que las bases de datos relacionales están optimizadas para el procesamiento de transacciones (Ver sección 3.1.1). Muchas aplicaciones comerciales, y multitud de aplicaciones personalizadas, usan un diseño habilitado para el uso de directorios.

AD LDS ofrece la mayoría de las funciones de ADS (y en realidad está basado en la misma base de código), aunque no exige la implementación de dominios ni de controladores de dominio.

AD LDS es similar a ADS en cuanto a que proporciona lo siguiente:

- Replicación con varios maestros.
- Compatibilidad con la interfaz de programación de aplicaciones (API) de interfaces del servicio Active Directory (ADSI).
- Particiones del directorio de aplicaciones.
- LDAP en Capa de sockets seguros (SSL).

Glosario

- **ADSL** (*Asymmetric Digital Subscriber Line* ó *Línea de abonado digital asimétrica*): es un tipo de tecnología de línea DSL. Consiste en una transmisión analógica de datos digitales apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado, siempre y cuando la longitud de línea no supere los 5,5 km medidos desde la Central Telefónica, o no haya otros servicios por el mismo cable que puedan interferir. Es una tecnología de acceso a Internet de banda ancha, lo que implica una velocidad superior a una conexión tradicional por módem en la transferencia de datos, ya que el módem utiliza la banda de voz y por tanto impide el servicio de voz mientras se use y viceversa. Esto se consigue mediante una modulación de las señales de datos en una banda de frecuencias más alta que la utilizada en las conversaciones telefónicas convencionales (300-3400 Hz), función que realiza el enrutador ADSL. Esta tecnología se denomina asimétrica debido a que la capacidad de descarga (desde la red hasta el usuario) y de subida de datos (en sentido inverso) no coinciden. La tecnología ADSL está diseñada para que la capacidad de bajada (descarga) sea mayor que la de subida, lo cual se corresponde con el uso de internet por parte de la mayoría de usuarios finales, que reciben más información de la que envían (o descargan más de lo que suben).

- **API** (*Application Programming Interface* ó *Interfaz de programación de aplicaciones*): es el conjunto de funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción. Son usadas generalmente en las bibliotecas (también denominadas vulgarmente "librerías").

- **bindRequest:** Se trata del primer mensaje enviado por un cliente a un servidor LDAP. Contiene la identificación del usuario y las credenciales, que pueden ser simples o sasl.

- **CCITT** (*Consultative Committee for International Telegraphy and Telephony* ó *Comité Consultivo Internacional Telegráfico y Telefónico*): antiguo nombre del comité de normalización de las telecomunicaciones dentro de la UIT (Unión Internacional de Telecomunicaciones) ahora conocido como UIT-T [34].

- **Centros Regionales:** Se trata de las oficinas más importantes que Senasa posee en el interior del país. Al ser un Organismo descentralizado, el país ha sido dividido en grandes centros (ver figura 2) donde cada uno de ellos juega un rol determinante para cada una de las regiones.

- **Controlador de dominio** (Domain controller)**:** Es un servidor que responde a requerimientos de autenticación de seguridad (inicio de sesión, chequeo de permisos, etc) dentro de un dominio de Windows Server. El dominio es un concepto introducido por Windows NT, en el cual a un usuario se le podía conceder acceso a los recursos asociados a una serie de equipos dentro de la red empleando un único usuario y contraseña.

- **DARPA** (*Defense Advanced Research Projects Agency* ó *Agencia de Investigación de Proyectos Avanzados de Defensa*) [35]: es una agencia del Departamento de Defensa de Estados Unidos responsable del desarrollo de nuevas tecnologías para uso militar. Fue creada en 1958 como consecuencia tecnológica de la llamada Guerra Fría, y del que surgieron, década después, los fundamentos de ARPANET, red que dio origen a Internet.

- **Distribuciones de Linux:** Una distribución Linux (coloquialmente llamada distro) es una distribución de software basada en el núcleo Linux que incluye determinados paquetes de software para satisfacer las necesidades de un grupo específico de usuarios, dando así origen a ediciones domésticas, empresariales y para servidores. Por lo general están compuestas, total o mayoritariamente, de software libre, aunque a menudo incorporan aplicaciones o controladores propietarios.

- **DNS** (*Domain Name System* ó *Sistema de Nombres de Dominio*): es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominio 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.

  La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS.

- **Dominio Active Directory:** Es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos (principalmente LDAP, DNS, DHCP, Kerberos). 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. Active Directory permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchas computadoras y aplicar actualizaciones críticas a una organización entera. 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.

- **Foreign Key** (*clave foránea o clave ajena*): En el contexto de bases de datos relacionales, es una limitación referencial entre dos tablas. La clave foránea identifica una columna o grupo de columnas en una tabla (tabla hija o referendo) que se refiere a una columna o grupo de columnas en otra tabla (tabla maestra o referenciada). Las columnas en la tabla referendo deben ser la clave primaria u otra clave candidata en la tabla referenciada.

  Los valores en una fila de las columnas referendo deben existir solo en una fila en la tabla referenciada. Así, una fila en la tabla referendo no puede contener valores que no existen en la tabla referenciada. De esta forma, las referencias pueden ser creadas para vincular o relacionar información. Esto es una parte esencial de la normalización de base de datos

- **FTP** (*File Transfer Protocol* ó *Protocolo de Transferencia de Archivos*) [36]: Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red IP, basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

  El servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21.

- **HTTP** (*Hypertext Transfer Protocol* ó *Protocolo de transferencia de hipertexto*) [37]: es el protocolo usado en cada transacción de la World Wide Web. HTTP fue desarrollado por el World Wide Web Consortium [38] y la Internet Engineering Task Force [39], colaboración que culminó en 1999 con la publicación de una serie de RFC, el más importante de ellos es el RFC 2616 que especifica la versión 1.1. HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Al cliente que efectúa la petición (un navegador web o un spider) se lo conoce como "user agent" (agente del usuario). A la información transmitida se la llama recurso y se la identifica mediante un localizador uniforme de recursos (URL). Los recursos pueden ser archivos, el resultado de la ejecución de un programa, una consulta a una base de datos, la traducción automática de un documento, etc.

- **IAB** (*Internet Architecture Board*) [40]: es el comité encargado de la supervisión del desarrollo técnico y de ingeniería de Internet por la Internet Society (ISOC) [41]. Supervisa una serie de grupos de trabajo, de los cuales los más importantes son la Internet Engineering Task Force (IETF) y la Internet Research Task Force (IRTF) [42].

- **IETF** (*Internet Engineering Task Force* ó *Grupo Especial sobre Ingeniería de Internet*) [39]: es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad. Fue creada en EE. UU. en 1986. La IETF es mundialmente conocida por ser la entidad que regula las propuestas y los estándares de Internet, conocidos como RFC.

  Es una institución sin fines de lucro y abierta a la participación de cualquier persona, cuyo objetivo es velar para que la arquitectura de Internet y los protocolos que la conforman funcionen correctamente. Se la considera como la organización con más autoridad para establecer modificaciones de los parámetros técnicos bajo los que funciona la red. La IETF se compone de técnicos y profesionales en el área de redes, tales como investigadores, integradores, diseñadores de red, administradores, vendedores, entre otros.

- **ISO** (*International Organization for Standardization* u *Organización Internacional de Normalización*) [43]: es el organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones (públicas o privadas) a nivel internacional.

  La ISO es una red de los institutos de normas nacionales de 163 países, sobre la base de un miembro por país, con una Secretaría Central en Ginebra (Suiza) que coordina el sistema. Está compuesta por delegaciones gubernamentales y no gubernamentales subdivididos en una serie de subcomités encargados de desarrollar las guías que contribuirán al mejoramiento.

- **ISP** (*Internet Service Provider* ó *Proveedor de Servicios de Internet*): es una empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, Cablemódem, GSM, Dial-up, Wifi, entre otros. Muchos ISP también ofrecen servicios relacionados con Internet, como el correo electrónico, alojamiento web, registro de dominios, servidores de noticias, etc.

- **Join:** En el contexto de bases de datos relacionales, refiere a combinar registros de dos o más tablas en una base de datos relacional.

- **Mbps:** Un megabit por segundo (Mb/s o Mbit/s) es una unidad que se usa para cuantificar un caudal de datos equivalente a 1 000 kb/s ó 1 000 000 b/s.

- **Metadirectorio**: Un sistema de metadirectorio proporciona el flujo de datos entre uno o más servicios de directorio y bases de datos, con el fin de mantener la sincronización de los datos, y es una parte fundamental de los sistemas de gestión de identidad. Los datos sincronizados son típicamente colecciones que contienen perfiles de usuario y posiblemente información de autenticación o de política. La mayoría de las implementaciones de

metadirectorio sincroniza datos en al menos un servidor de directorio basado en LDAP, para asegurar que las aplicaciones basadas en LDAP tengan acceso a los datos.

- **MPLS:** (*Multiprotocol Label Switching*) es un mecanismo en las redes de telecomunicaciones de alto rendimiento que transmite los datos de un nodo de red al siguiente basado en etiquetas cortas en lugar de largas direcciones de red, evitando búsquedas complejas en una tabla de enrutamiento. Las etiquetas identifican enlaces virtuales (rutas) entre los nodos distantes en lugar de puntos finales. MPLS puede encapsular los paquetes de varios protocolos de red. MPLS es compatible con una amplia gama de tecnologías de acceso, incluidos T1/E1, ATM, Frame Relay y DSL.

- **NTP** (*Network Time Protocol*) [44]: es un protocolo de red para la sincronización de reloj entre los sistemas informáticos a través de redes de datos de conmutación de paquetes con latencia variable.

- **Proxy:** Es un programa o dispositivo que realiza una acción en representación de otro, esto es, si 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: proporcionar caché, control de acceso, registro del tráfico, prohibir cierto tipo de tráfico etc.

  Su finalidad más habitual es la de servidor proxy, que consiste en interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc. Esta función de servidor proxy puede ser realizada por un programa o dispositivo.

- **RFC** (*Request for Comments* ó *Petición De Comentarios*): son una serie de notas sobre Internet, y sobre sistemas que se conectan a internet, que comenzaron a publicarse en 1969. Cada una de ellas individualmente es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet (originalmente de ARPANET), que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.

  Cualquiera puede enviar una propuesta de RFC a la IETF, pero es ésta la que decide finalmente si el documento se convierte en una RFC o no. Si luego resulta lo suficientemente interesante, puede llegar a convertirse en un estándar de Internet.
  Cada RFC tiene un título y un número asignado, que no puede repetirse ni eliminarse aunque el documento se quede obsoleto.
  Cada protocolo de los que hoy existen en Internet tiene asociado un RFC que lo define, y posiblemente otros RFC adicionales que lo amplían.

- **Rollback:** En tecnologías de base de datos, un rollback es una operación que devuelve a la base de datos a algún estado previo. Los Rollbacks son importantes para la integridad de la

base de datos, a causa de que significan que la base de datos puede ser restaurada a una copia limpia incluso después de que se han realizado operaciones erróneas. Son cruciales para la recuperación de crashes de un servidor de base de datos; realizando rollback (devuelto) cualquier transacción que estuviera activa en el tiempo del crash, la base de datos es restaurada a un estado consistente.

- **SearchRequest:** Utilidad que localiza y recupera las entradas de un directorio LDAP. Esta utilidad abre una conexión con el servidor especificado utilizando el nombre completo y la contraseña y localiza entradas en el servidor LDA en base a filtros de búsqueda especificados. Los ámbitos de búsqueda pueden incluir una sola entrada, subentradas inmediatas de una entrada, un árbol completo o un subárbol.

- **SQL** (*Structured Query Language* ó *Lenguaje de Consulta Estructurado*): es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ellas. Una de sus características es el manejo del álgebra y el cálculo relacional que permiten efectuar consultas con el fin de recuperar de forma sencilla información de interés de bases de datos, así como hacer cambios en ella.

Referencias

[1] http://www.senasa.gob.ar. Página oficial de Senasa.

[2] Sistema de Nombres de Dominio DNS. http://www.zoneedit.com/doc/rfc/ RFCs relacionadas.

[3] X.500, http://www.x500standard.com/ Sitio de la comunidad del estándar X.500.

[4] RFC 1202, Directory Assistance Service. http://datatracker.ietf.org/doc/rfc1202/

[5] RFC 1249, DIXIE Protocol Specification. http://datatracker.ietf.org/doc/rfc1249/

[6] RFC 1487, X.500 Lightweight Directory Access Protocol. http://datatracker.ietf.org/doc/rfc1487/

[7] RFC 1777, Lightweight Directory Access Protocol. http://datatracker.ietf.org/doc/rfc1777/

[8] RFC 1778, *The String Representation of Standard Attribute Syntaxes*. http://datatracker.ietf.org/doc/rfc1778/

[9] RFC 1779, *A String Representation of Distinguished Names*. http://datatracker.ietf.org/doc/rfc1779/

[10] RFC 1959, *An LDAP URL Format*. http://datatracker.ietf.org/doc/rfc1959/

[11] RFC 1960, *A String Representation of LDAP Search Filters*. http://datatracker.ietf.org/doc/rfc1960/

[12] RFC 2251, *Lightweight Directory Access Protocol (v3)*. http://datatracker.ietf.org/doc/rfc2251/

[13] RFC 2252, *Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions*. http://datatracker.ietf.org/doc/rfc2252/

[14] RFC 2253, *Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names*. http://datatracker.ietf.org/doc/rfc2253/

[15] RFC 2254, *The String Representation of LDAP Search Filters*. http://datatracker.ietf.org/doc/rfc2254/

[16] RFC 2255, *The LDAP URL Format*. http://datatracker.ietf.org/doc/rfc2255/

[17] RFC 2256, *A Summary of the X.500(96) User Schema for use with LDAPv3*. http://datatracker.ietf.org/doc/rfc2256/

[18] RFC 2829, *Authentication Methods for LDAP*. http://datatracker.ietf.org/doc/rfc2829/

[19] RFC 2830, *Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security*. http://datatracker.ietf.org/doc/rfc2830/

[20] RFC 3377, *Lightweight Directory Access Protocol (v3): Technical Specification*. http://datatracker.ietf.org/doc/rfc3377/

[21] SASL RFC 4422, *Simple Authentication and Security Layer (SASL)*. http://datatracker.ietf.org/doc/rfc4422/

[22] Organizational Unit, http://en.wikipedia.org/wiki/Organizational_Unit

[23] http://minagri.gob.ar. Página oficial del *Ministerio de Agricultura Ganadería y Pesca de la Nación*.

[24] http://sinavimo.senasa.gob.ar. Sistema Nacional Argentino de Vigilancia y Monitoreo de Plagas (dependiente de Senasa).

[25] http://www.microsoft.com. Página oficial de Microsoft.

[26] http://www.openldap.org/. Página oficial del proyecto OpenLDAP.

[27] http://www.samba.org/. Página oficial del proyecto Samba.

[28] http://www.microsoft.com/conosur/hechos/studies.mspx. Lista de casos de éxito de implementaciones a gran escala sobre plataformas Microsoft Active Directory.

[29] Referencias para el diseño y configuración de Microsoft Active Directory:

- Planeamiento de Active Directory en un entorno de oficinas remotas: http://technet.microsoft.com/en-us/library/cc749944.aspx
- Diseño de un dominio con Active Directory http://www.informit.com/articles/article.aspx?p=32080&seqNum=6 http://technet.microsoft.com/en-us/library/bb727085.aspx
- Sitios y Servicios http://www.microsoft.com/latam/technet/productos/windows/windowsserver2003/adsrv.mspx

[30] Referencias para el diseño y configuración de Active Directory Lightweight Directory Service:

- http://www.microsoft.com/spain/windowsserver2008/roles/apps_lds.mspx
- http://technet.microsoft.com/en-us/library/cc754361%28WS.10%29.aspx
- http://blogs.technet.com/b/idaguys/archive/2009/06/19/overiview-of-authentication-in-ad-lds.aspx
- http://www.windowsnetworking.com/articles_tutorials/Configuring-Active-Directory-Lightweight-Directory-Service-Part1.html

[31] http://inta.gob.ar/. Página oficial del *INTA*

[32] DHCP en Wikipedia. http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

[33] Kerberos en Wikipedia. http://en.wikipedia.org/wiki/Kerberos_%28protocol%29

[34] http://www.itu.int/ITU-T/. Página oficial de *ITU-T*.

[35] http://www.darpa.mil/. Página oficial de *DARPA*.

[36] RFC 959, *FILE TRANSFER PROTOCOL (FTP)*. http://www.ietf.org/rfc/rfc959.txt

[37] RFC 2616, *Hypertext Transfer Protocol -- HTTP/1.1*. http://www.w3.org/Protocols/rfc2616/rfc2616.html

[38] http://www.w3.org/. Página oficial del *World Wide Web Consortium*.

[39] http://www.ietf.org/. Página oficial de *Internet Engineering Task Force*.

[40] http://www.iab.org/. Página oficial de *Internet Architecture Board* .

[41] http://www.internetsociety.org/es. Página oficial de Internet Society (ISOC)

[42] http://irtf.org/. Página oficial de *Internet Research Task Force (IRTF)*

[43] http://www.iso.org/iso/home.html. Página oficial de *ISO International Organization for Standardization*.

[44] NTP D.L. Mills. Network Time Protocol (NTP). RFC 958, September 1985. Obsoleta por RFCs 1059, 1119, 1305.

Bibliografía adicional

- James F. Kurose. Redes de Computadoras. Un enfoque descendente. 2010. ISBN 978-84-7829-119-9.
- Gerald Carter. LDAP System Administration. Marzo 2003. ISBN 978-1-56592-491-8.
- Dan Holme, Nelson Ruest, Danielle Ruest. Configuring Windows Server 2008 Active Directory. ISBN 978-0-7356-2513-6.
- Orin Thomas, John Policelli, Ian McLean, J.C. Mackin Paul Mancuso, David R. Miller. Windows Server Enterprise Administration. ISBN 978-0-7356-2509-9.
- Steven Tuttle, Ami Ehlenberger, Ramakrishna Gorthi, Jay Leiserson, Richard Macbeth, Nathan Owen, Sunil Ranahandola, Michael Storrs, Chunhui Yang. Understanding LDAP. Design and Implementation. ISBN 073849786X. Junio de 2004.