UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISENO DE UNA RED DE COMUNICACIONES PARA UNA ENTIDAD PUBLICA QUE BRINDA EL SERVICIO DE TIMESTAMPING

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

CIRO PEÑA DUEÑAS

PROMOCION

2007-I

LIMA-PERU

2012

DISEÑO DE UNA RED DE COMUNICACIONES PARA UNA ENTIDAD PUBLICA QUE BRINDA EL SERVICIO DE TIMESTAMPING

DEDICATORIA:

A Dios, por brindarme buena salud.

A mis madres, porque siempre están conmigo.

A mi padre Falconieri que siempre me apoya y aconseja.

A Valentina que me dio la responsabilidad más hermosa de este mundo

A mi hijo Leonardo su solo existencia representa el éxito.

A mi querida Universidad, mi alma mater.

SUMARIO

El presente trabajo está enfocado en realizar el diseño de una red de comunicaciones para una entidad que tiene por objetivo brindar el servicio de sello de tiempo (time stamping en inglés).

El primer objetivo de este trabajo consiste en especificar cuál son los equipos más adecuados para la red de comunicaciones de la entidad pública (también puede ser aplicada también a entidad privadas) para que brinde el servicio de sello de tiempo, tal que garantice los criterios de alta disponibilidad, redundancia y balanceo de carga.

El segundo objetivo es diseñar el proceso de operación del servicio de sello de tiempo.

El tercer objetivo es identificar los pasos que debe seguir una entidad para lograr la acreditación como SVA prestadora del servicio de sello de tiempo ya que sin el cumplimiento de este requerimiento no se puede brindar el servicio de sello de tiempo a las personas naturales y jurídicas.

El cuarto objetivo es dar a conocer la firma digital, el sello de tiempo y el beneficio de las mismas en las transacciones electrónicas de un ciudadano.

El quinto objetivo es hacer de conocimiento que existe en la legislación peruana mecanismos que regulan la utilización de la firma digital otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita, basado en estos principios legales el servicio de sello de tiempo puede ser brindado al amparo de la ley peruana.

ÍNDICE

INTRODUCCIÓN

Según el estudio elaborado por IESE Business School y EVERIS, el Indicador Tecnologías de la Información y las Comunicaciones (TIC) para el 2011 en Perú se ha incrementado un 11.2%[1] respecto al año pasado, el uso de las redes sociales ha tenido una variación interanual de 147% (190 cada mil personas), el número de usuarios de Internet crece a un 8.1% anual (351 por cada mil habitantes), la compra de computadoras crece a un 20,9% interanual con 173 unidades por cada mil personas. Estas impresionantes estadísticas nos demuestra que cada vez más personas se relacionan e interrelacionan con la tecnología y el internet, pero el incremento del uso de internet por parte de las personas no solamente es para búsqueda de información, también con lleva a la necesidad de querer realizar transacciones a través del mismo[2], tales como comercio electrónico, acceso información, tramites con organismos del Estado Peruano, etc.; esto por las características propias del internet, tales como: la facilidad de uso, el intercambio de información y el ahorro de tiempo en las transacciones; pero hay que tener en cuenta que el internet está abierto a cualquiera que tenga una conexión a la misma, y esto conlleva a la aparición de amenazas tales como, robo de información, suplantación de identidad, modificación de información, fraude electrónico, etc., lo cual genera mucha desconfianza en las personas para llevar a cabo sus transacciones electrónicas por internet, y más aún si estas involucran un intercambio financiero entre las partes. Después de un análisis del problema se ha identificado que la confianza en los servicios ofrecidos es un elemento crítico para que las personas puedan realizar transacciones por internet, para que esto pueda darse es necesario evitar las amenazas arriba mencionadas, y asegurar todo el proceso de intercambio de información que fluye durante el tiempo que dure la transacción, para poder lograr esto se debe cumplir con estos conceptos:

1. **Integridad de la información:** La información que es publicada y compartida no puede ser alterada, por ningún mecanismo.
2. **Confidencialidad de la información:** Cuando solamente las personas autorizadas pueden obtener y acceder a esta información, y en caso una persona no autorizada obtuviera esta información (independiente de la forma) esta no podrá ser accedida.
3. **Disponibilidad de la Información:** La información debe estar disponible en el momento que se necesite.

4. **No repudio:** La información no puede ser negada por el autor de la misma
5. **Hora exacta**: La información debe ser válida en la fecha y hora exacta sin posibilidad de duda ni cuestionamiento

Si se hace uso del certificado digital, la clave pública, clave privada, mecanismo de sello de tiempo, software de firma digital y el procedimiento cifrado entonces se puede obtener:

1. Confidencialidad. Los documentos confidenciales, pueden ser protegidos por medio de técnicas sofisticadas de cifrado, cuando se envíen a través de redes públicas como Internet.
2. No repudio: El autor del documento puede ser confirmado positivamente por medio del uso de la firma digital y cifrado (usando la clave pública y clave privada).
3. Integridad: Las técnicas de cifrado pueden ser aplicadas para asegurar que los documentos electrónicos no han sido alterados o dañados durante una transmisión y puede ser usado para proveer una firma digital segura.
4. Hora exacta: Se puede vincular un documento electrónico con una fecha y hora exacta al momento de su emisión mediante el uso del sello de tiempo, evitando cualquier duda sobre el momento de generación del mismo.
5. Disponibilidad: Mediante un diseño e implementación adecuado de una infraestructura de soporte (especialmente una red de comunicaciones) se puede asegurar que aun en caso de ataques hostiles el servicio, documentos, etc., estará siempre disponible para quien lo solicite.

De lo expuesto líneas arriba se puede inferir que con el uso del certificado digital, la clave pública, clave privada, mecanismo de sello de tiempo, software de firma digital, procedimiento cifrado y infraestructura adecuada se puede asegurar el intercambio de información a través de internet y con ello obtener la confianza de los usuarios en los servicios ofrecidos.

En nuestro país existen muy pocas instituciones que brindan el servicio de sello de tiempo (ninguna de ellas con acreditación ante INDECOPI [3]) funcionando el servicio de manera privada, aislada, estando fuera del narco jurídico, lo cual hace que estas transacciones electrónicas a través de internet estén basadas en acuerdos privados de reconocimiento, sin valor jurídico, y con la consecuente duda sobre si la transacción realizada es confiable o segura.

Es así que el objetivo del presente trabajo es realizar el diseño de una red de comunicaciones para cumplir con los conceptos de integridad, confidencialidad, disponibilidad y hora exacta, para brindar el servicio de sello de tiempo en la transacciones electrónicas de una institución pública y con esto generar la confianza necesaria para que cuando una persona acceda al internet pueda realizar trámites de

diversa índole (tramites con el Estado, comercio electrónico, etc.) con total confianza, ya que su identidad no será suplantada, el proceso que realiza no se perderá ni tendrá tiempos de espera y se tendrá total certeza que la firma del documento se realizó en la hora y fecha correcta sin posibilidad de alteración o duda del mismo.

No es objetivo del presente trabajo la realización de pruebas, ni de la implementación del diseño de red propuesto.

CAPITULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

En este capítulo se describe el problema objeto de este informe.

1.1 Descripción del problema

Cuando se quiere realizar una transacción electrónica por internet, intervienen dos actores, el emisor y el receptor, estos interactúan de tal forma que mediante acuerdos preestablecidos pueden llegar a establecer un flujo de información, los actores pueden ser persona-empresa, persona-persona, persona-gobierno, etc., y el uso del mismo puede ser:

- Acceder a servicios de comercio electrónico,
- Pago de impuestos,
- Pago se servicios,
- Acceso a información personal, etc.,

Como resultado de estas transacciones electrónicas se genera un documento electrónico, el cual para asegurar que la información contenida en el mismo es confiable y verdadera debe contener una firma digital, pero para asegurar que el documento existió en un momento dado, es necesario contar con un mecanismo que indique la fecha y hora en la cual se realizó el proceso de firma digital, este mecanismo debe ser confiable y debe asegurar que la firma digital del documento electrónico se realizó en la fecha y hora indicadas, las características a cumplir de este mecanismo son:

- Ser confiable.
- Ser imparcial.
- Brindar la fecha y hora exacta.
- Integrar procesos de firma digital.
- Estar disponible a toda hora.

El cumplimiento de estas características solo puede ser realizado a través del mecanismo de sello de tiempo, y este servicio debe ser brindado por un tercero de confianza, para el caso peruano se denomina Prestador de Servicios de Valor Añadido (SVA);para que una SVA brinde el servicio de sello de tiempo debe disponer de una infraestructura y una red de comunicaciones que nos asegure que este mecanismo va a funcionar con criterios de disponibilidad, seguridad y redundancia, además deber ser acreditado ante INDECOPI como Prestador del Servicio de Valor Añadido (SVA), este

proceso de acreditación en la actualizad es en sí una incógnita ya que no existe entidad peruana alguna que tenga esta acreditación.

1.2 Situación actual

Muchos de los servicios (procesos de trámites, solicitudes, etc.) que se brindan en la actualidad a nivel de persona-gobierno (entiéndase por tanto para persona natural como para persona jurídica) son realizados de forma presencial, lo cual implica una inversión de tiempo y costos asociados que se incurren tanto al utilizar y al brindar el servicio, algunas de las características de estos servicios son:

- Largas colas de espera,
- Pérdida de tiempo
- Perdida de dinero,
- Límite de horario de atención, etc.

Además como estos servicios requieren el uso de documentación impresa, se requiere personal dedicado a la recepción de documentos, verificación de firmas autorizadas, digitalización de documentos, control de calidad, fotocopiado, etc, como consecuencia de esto se generan costos directos , tales como:

- Costos operativos
- Costos de personal procesa la documentación
- Costos de procesos de control,
- Costos de procesos supervisión
- Costos de procesos de verificación
- Costos de evaluación de requisitos de documentación, etc.

Lo indicado líneas arriba hace que se incrementen los costos del servicio y como consecuencia directa también se incrementa la burocracia, ya que es necesario incrementar el personal para la realización de las actividades relacionadas. Además durante todo el tiempo que dura la prestación del servicio existe la dependencia del documento físico, como consecuencia de esto se incurren en costos indirectos relacionados al proceso tales como:

a. Desde el punto de vista del usuario:

- Costo de movilidad, ya que hay que firmar documentos de forma presencial.
- Costo por el tiempo de espera, para poder ingresar a las instalaciones.
- Costo de utilización de medios impresos (fotocopias, solicitudes, etc.)

b. Desde el punto de vista la entidad que brinda el servicio:

- Costo de servicio de seguridad
- Costo por el uso de servicios básicos (luz y agua), etc.

Todo este genera un círculo vicioso ya que si se desea brindar un servicio con calidad, se requiere más personal, lo que conlleva a la necesidad de requerir una infraestructura más costosa y esto trae como consecuencia incrementar los costos del servicio a la persona, que a su vez demanda más calidad por el servicio que paga y así sucesivamente.

1.2.1 Análisis de un trámite actual

Se va a analizar el trámite duplicado de DNI (Ver Tabla Nº1.1) ofrecido por el Estado Peruano en el portal de servicios al ciudadano [4].

TABLA Nº 1.1: Proceso de solicitud de duplicado de DNI

N°	Actividad	Costos asociados
1	-Movilizarse al Banco de Nación más cercana -Realizar cola. -Pagar el recibo. -Recepcionar recibo.	-Movilidad -Horas/hombre -Pago por recibo (documento impreso) -Costos de personal de atención
2	-Movilizarse a la agencia -Realizar cola. -Sacar ticket de atención. -Presentar recibo del Banco de la Nación. -Rellenar ficha registral -Firmar la ficha registral. -Presentar la Ficha Registral. -Recepcionar documento desglosable (documento donde se indica la fecha de entrega de DNI) Firmar ficha registral. Retirarse de la agencia	-Movilidad -Horas/hombre -Impresión de documentos -Costos de personal de atención
3	Esperar hasta la fecha de entrega	Ninguno
4	-Regresar a la agencia -Realizar cola. -Presentan documento desglosable -Firmar documento de entrega de DNI. -Salir de la agencia	-Movilidad -Horas/hombre -Costos de personal de atención

Como se puede observar, las características de este trámite son: costos directos por movilidad, altos costos de personal de atención, altos valores de tiempo invertido en el proceso, largas colas de espera, como consecuencia de todo esto existe pérdida de tiempo y dinero, los cuales son asumidos tanto por ciudadano como por el Estado Peruano.

CAPÍTULO II
NORMATIVA VIGENTE

En este capítulo se describen las leyes, decretos supremos, normas que ha establecido el Estado Peruano para el uso de los certificados digitales, firmas digitales y mecanismos de sello de tiempo.

2.1 Leyes

2.1.1 Ley Nº 27269, Ley de Firmas y Certificados Digitales

La Ley Nº 27269, Ley de Firmas y Certificados Digitales, modificada por la Ley Nº27310 tiene por objeto regular la utilización de la firma digital otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad. Se entiende por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita. Esta ley se aplica a aquellas firmas digitales que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos, puedan vincular e identificar al firmante, así como garantizar la autenticación e integridad de los documentos electrónicos.

2.1.2 Ley Nº 27444, Ley del Procedimiento Administrativo General, y sus modificaciones.

La Ley Nº 27444, Ley del Procedimiento Administrativo General, y sus modificaciones regulan las actuaciones de la función administrativa del Estado y el procedimiento administrativo común desarrollados en las entidades.

Las Entidades del Estado deben cumplir con los principios administrativos, así como los derechos y deberes de los sujetos del procedimiento, establecidos en la presente Ley, algunos de los cuales son:

- Principio de imparcialidad
- Principio de presunción de veracidad, etc

2.1.3 Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado.

Esta Ley declara al Estado peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y construir un Estado democrático, descentralizado y al

servicio del ciudadano, y tiene por objeto establecer los principios y la base legal para iniciar el proceso de modernización de la gestión del Estado, en todas sus instituciones e instancias.

El proceso de modernización de la gestión del Estado tiene como finalidad fundamental la obtención de mayores niveles de eficiencia del aparato estatal, de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos.

Una de las acciones para la modernización del Estado es lograr una mayor eficiencia en la utilización de los recursos del Estado, por lo tanto, se debe eliminar la duplicidad o superposición de competencias, funciones y atribuciones entre sectores y entidades o entre funcionarios y servidores.

Además el Estado debe promover y establecer los mecanismos para lograr una adecuada democracia participativa de los ciudadanos, a través de mecanismos directos e indirectos de participación.

2.2 Decretos supremos

2.2.1 Decreto Supremo Nº 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales y su modificatoria.

El presente Reglamento regula la utilización de firmas electrónicas en mensaje de datos y documentos electrónicos, generadas bajo la Infraestructura Oficial de Firma Electrónica comprendiendo el régimen de acreditación y supervisión de las entidades de certificación, así como de las entidades de registro o verificación, establecidas. Cualquier otra firma electrónica podrá tener los mismos efectos que los de las firmas generadas bajo la Infraestructura Oficial de Firma Electrónica, siempre que la autoridad administrativa competente (INDECOPI) apruebe mediante los mecanismos adecuados su uso.

2.2.2 Decreto Supremo Nº 070-2011-PCM

El Decreto Supremo Nº 070-2011-PCM modifica Decreto Supremo Nº 052-2008-PCM, para reconocer a los certificados digitales emitidos por el Registro Nacional de Identificación y Estado Civil (RENIEC) en tanto dicha entidad no se encuentre acreditada ante la Autoridad Administrativa Competente, esto es, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI).

2.3 Guías de acreditación

2.3.1 Guía de Acreditación para Prestadoras de Servicios de Valor Añadido.

Establece los procedimientos y criterios que deben cumplir los Prestadores de Servicios de Valor Añadido (SVA) para lograr su acreditación ante la Autoridad Administrativa Competente.

Un servicio de valor añadido es el sello de tiempo (estándares de Time Stamp RFC 3161 y RFC 3628) y también los mecanismos de seguridad para prevenir cualquier cambio intencional en los documentos archivados, tales como el uso de resúmenes (hashes).

2.3.2 Guía de Acreditación de Entidades de Registro ER.

Este documento establece los procedimientos y criterios que deben cumplir las Entidades de Registro (ER) para lograr su acreditación ante INDECOPI, el cual ha sido designado como la Autoridad Administrativa Competente (AAC), además establece los requisitos y pautas que buscan asegurar que la Entidad de Registro (ER) que pretenda operar dentro de la Infraestructura Oficial de Firma Electrónica (IOFE) cumpla determinados niveles de seguridad e interoperabilidad a efectos de poder obtener la correspondiente acreditación.

2.3.3 Guía de Acreditación de Entidades de Certificación EC.

Este documento establece los procedimientos y criterios que deben cumplir las Entidades de Certificación (EC) para lograr la Acreditación de la EC.

La Autoridad Administrativa Competente (AAC), establece los requisitos y pautas que buscan asegurar que la Entidad Certificadora (EC) que pretenda operar dentro de la Infraestructura Oficial de Firma Electrónica (IOFE) cumpla determinados niveles de seguridad e interoperabilidad a efectos de poder obtener la correspondiente acreditación. Los criterios para el funcionamiento de la EC se basan en estándares internacionalmente aceptados (tales como la RFC 3280) y en los principios acordados en la denominada Declaración de Lima, suscrita en el Sexto Meeting Ministerial del APEC llevado a cabo en Lima del 1° al 3 de julio del año 2005 [4].

La Guía de Acreditación de Entidades de Certificación EC debe ser empleado por las EC; con el objetivo que puedan identificar los requisitos necesarios que deben cumplir.

2.3.4 Guía de Acreditación de Software para Firmas Digitales.

Este documento describe los requerimientos que permiten que las aplicaciones de software empleen la tecnología de clave pública (Public Key, PK) e interactúen con la Infraestructura de Clave Pública (Public Key Infraestructura, PKI) establecida por la Infraestructura Oficial de Firma Electrónica (IOFE).

CAPÍTULO III
MARCO TEÓRICO

En este capítulo se describen el fundamento teórico de las tecnologías que se van a usar para el cumplimiento de los objetivos del informe.

3.1 Gobierno Electrónico

Consiste en el uso de las tecnologías de la información para la interacción del gobierno con las personas naturales (ciudadanos), así como también con las personas jurídicas, con el objetivo brindar información y mejorar los servicios ofrecidos a las personas, aumentar la eficiencia y eficacia de la gestión pública e incrementar sustantivamente la trasparencia del sector público e incrementar la participación ciudadana.

3.1.1 Evolución del Gobierno Electrónico

El Internet y las tecnologías basadas en web ofrecen posibilidades reales de transformación de las interacciones entre el Estado y la sociedad en contraste a las tecnologías anteriores que fueron orientadas de manera exclusiva a un grupo exclusivo de privilegiados que tenían acceso a las mismas. La evolución del gobierno electrónico ha seguido el siguiente camino:

- Burocracia con base de dato y redes de PC,
- después burocracia con uso masivo de computadoras,
- seguido de burocracia con introducción de TI,
- y ahora tenemos burocracia con gobierno en la web

Dado el interés actual del gobierno de acercarse a las personas, en la actualidad nos encontramos en la etapa de "gobierno en la web" (Ver Fig. 3.1) que no es otra cosa que el uso por parte del Estado de las tecnologías de la Información (TI) particularmente las tecnologías web (portales, servicios en línea, etc.), para poner al alcance de los ciudadanos los medios electrónicos necesarios y suficientes para poder interactuar con el Estado, la aplicación del uso de estas tecnologías es a través de los servicios en línea tales como:

- pago de facturas electrónicas,
- pago de impuestos,
- consulta a base de datos nacionales,
- separación de citas de atención medica, etc.

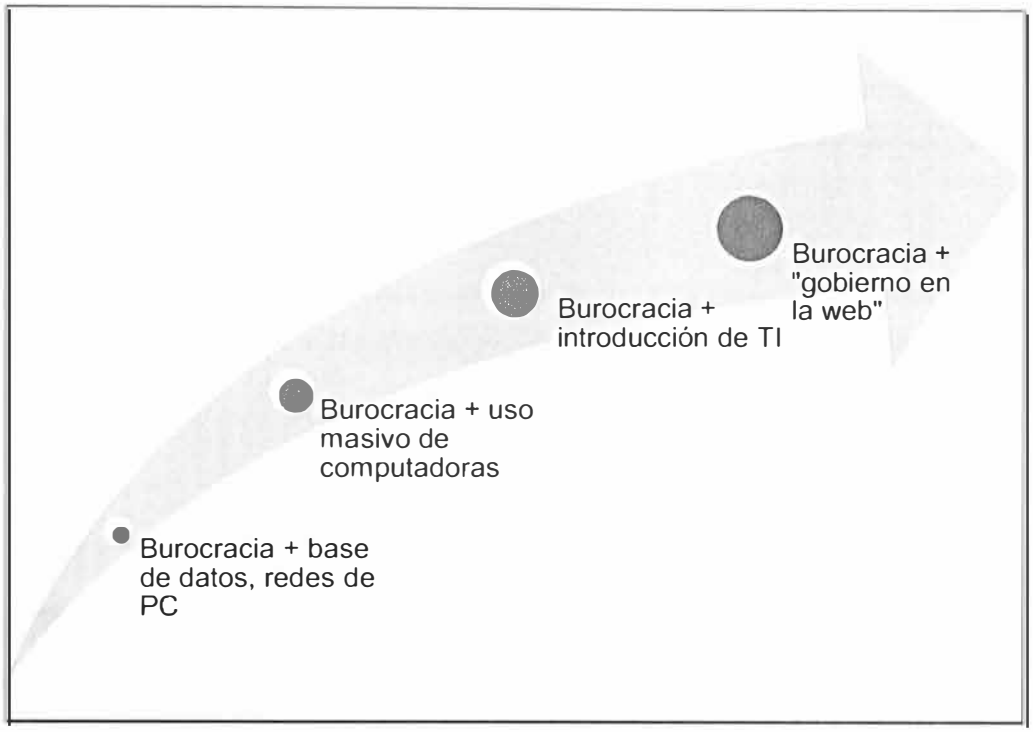


Fig. 3.1 Evolución del Gobierno electrónico

3.1.2 Características del e-Gobierno

Algunas de las características del e-gobierno actual son:

a. Los ciudadanos deben ser incentivados a utilizar el e-gobierno, pero actualmente existen brechas digitales, porque hay grupos que no tienen acceso a la web (ver TABLA Nº 3.1).

TABLA Nº 3.1 Frecuencia de uso de internet

¿Con qué frecuencia hace usted uso de Internet?			
	Agosto 2008	Setiembre 2009	Junio 2010
Todos los días o casi todos los días	26	28	25
Dos a tres veces por semana	21	15	17
Dos a tres veces por mes	7	6	5
Dos a una vez al mes	5	4	3
Con menor frecuencia	10	8	7
Nunca	31	39	41
No precisa	0.2	-	2
Total %	**100**	**100**	**100**
Base de entrevistas	534	511	477

b. Uso masivo de hardware y software.
c. Modificación de patrones de conducta social (uso de redes sociales).
d. El gobierno tiende a ser más transparente pero puede ser más complejo, confuso y difícil de controlar.
e. El gobierno lucha por mantener los conocimientos técnicos (y competir con el sector privado en habilidades).
f. Externalizar gran parte de la administración electrónica.
g. Los ciudadanos interactúan más con organizaciones comerciales que con el gobierno (a veces por paradigmas basadas en experiencias pasadas).

3.2 Infraestructura de llave publica- PKI

Una infraestructura de llave pública (PKI, Public Key Infrastructure en inglés) es un sistema, que hace posible la seguridad y el no repudio en transacciones financieras y el intercambio de información sensible entre dos actores (personas, instituciones, gobierno, etc.).

Una PKI administrará la generación y distribución de llaves públicas y privadas; y publicará las llaves públicas con la identificación de los usuarios en repositorios de clave pública. Una PKI provee un alto grado de confianza, manteniendo las claves privadas seguras, las claves públicas se conectan a sus respectivas claves privadas, y el par de claves públicas y privadas aseguran la veracidad de la persona quien dice ser.

Los criterios de una PKI se basan en estándares internacionalmente aceptados y en los principios acordados en la denominada Declaración de Lima, suscrita en el Sexto Meeting Ministerial del APEC[6]

En nuestro país ha sido designada como Autoridad Administrativa Competente (AAC) el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual INDECOPI, específicamente la Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias.

Una PKI (Infraestructura de clave pública)tiene los siguientes componentes (ver Fig. 3.2):

- Autoridad Administrativa Competente (AAC).
- Entidad de certificación (EC).
- Entidad de registro (ER).
- Prestadora de servicios de valor añadido (SVA)
- Certificado digital.
- Procedimiento de ciclo de vida de certificados (Emisión, re-emisión, revocación).
- Mecanismo de Sello de Tiempo.
- Procedimiento de Sello de Tiempo.
- Software de firma digital.

- Mecanismos de verificación del estado del certificado (CRL, OSCP).
- Repositorio de certificados.

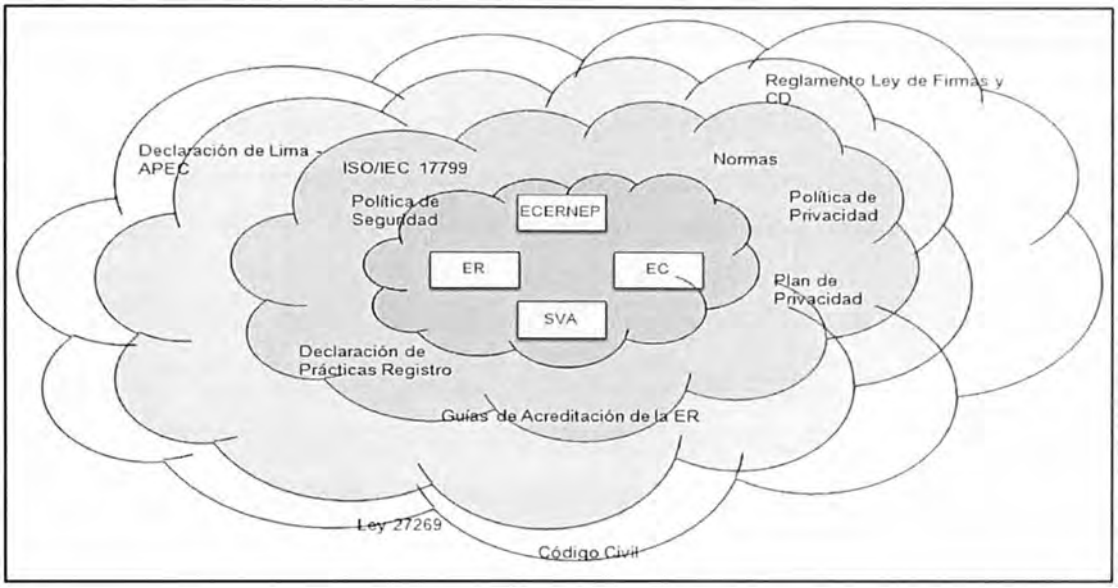


Fig. 3.2 Componentes de la PKI

3.2.1 Entidad de Certificación-EC

Es una entidad de confianza con personería jurídica pública o privada que presta indistintamente servicios de emisión, cancelación u otros servicios inherentes a la certificación digital. La Entidad de Certificación legitima ante los terceros que confían en sus certificados la relación entre la identidad de un usuario y su clave pública. La confianza de los usuarios en la EC (Entidad de Certificación) es importante para el funcionamiento del servicio y justifica el empleo de la misma.

3.2.2 Prestador de Servicios de Valor Añadido–SVA

Es una entidad de confianza con personería jurídica, que presta servicios de valor añadido tales como sello de tiempo y otros. Las aplicaciones de la SVA deben previamente pasar un proceso de acreditación ante INDECOPI. Son supervisadas y reguladas por la normatividad vigente.

3.2.3 Entidad de Registro-ER

Es una entidad de confianza con personería jurídica, con excepción de los notarios públicos, encargada del levantamiento de datos, comprobación de éstos respecto a un solicitante de un mecanismo de firma electrónica o certificación digital, la aceptación y autorización de las solicitudes para la emisión de un mecanismo de firma electrónica o certificados digitales, así como de la aceptación y autorización de las solicitudes de cancelación de mecanismos de firma electrónica o certificados digitales. Son supervisadas y reguladas por la normatividad vigente.

3.3 Función Hash

Una función hash es una función que hace posible obtener un hash (también llamado resumen de mensaje) de un texto, es decir, obtener una serie corta de caracteres que

representan el texto al cual se le aplica esta función hash. La función hash asocia de manera única un hash con un texto plano (ver Fig. 3.3) la propiedad de este hash es que la mínima modificación del documento causará una modificación en el hash (esta propiedad es fundamental para la firma digital).

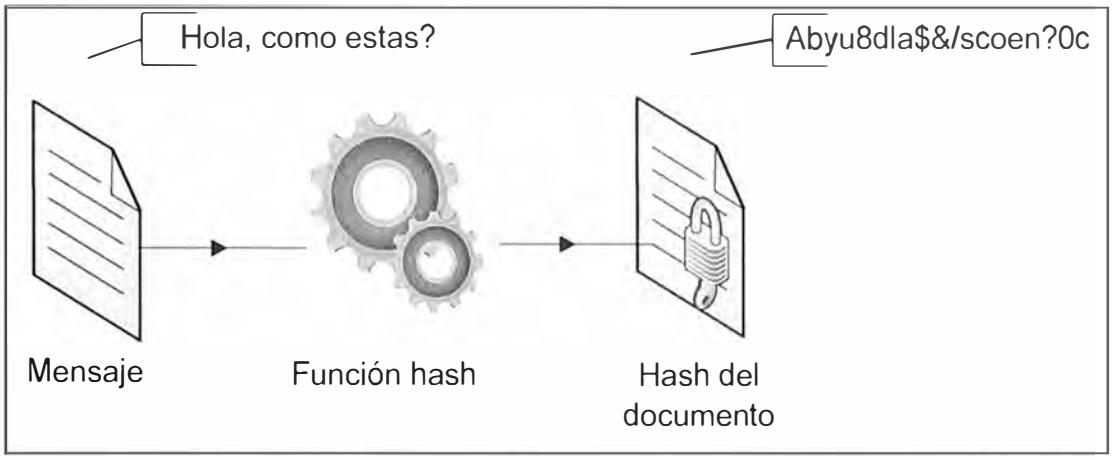


Fig. 3.3: Operación de la Función hash

Otra propiedad de la función hash es que es unidireccional, esto quiere decir que no hay manera de reconstruir el texto plano a partir del hash (ver Fig. 3.4). Por esta propiedad puede decirse que la función hash representa la huella digital de un documento, ya que es único para cada documento.

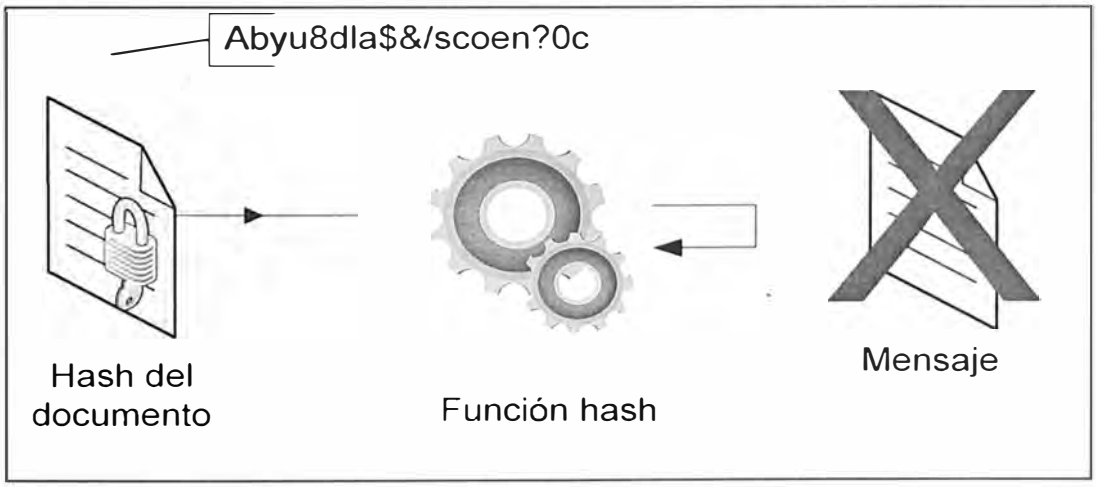


Fig. 3.4: Colisión de Operación

3.3.1 Algoritmos más usados

Los algoritmos hash más utilizados en la actualidad son:

- MD5 (MD que significa Message Digest; en castellano, Resumen de mensaje). Desarrollado por Rivest en 1991, el MD5 crea, a partir de un texto, una huella digital de 128 bits procesándola en bloques de 512 bits. Es común observar documentos descargados de Internet que vienen acompañados por archivos MD5: este es el hash del documento que hace posible verificar su integridad.
- SHA (Secure Hash Algorithm; en castellano, Algoritmo Hash Seguro) crea una huella digital que tiene 160 bits de longitud.

- SHA-1 es una versión mejorada de SHA que data de 1994. Produce una huella digital de 160 bits a partir de un mensaje que tiene una longitud máxima de 264 bits y los procesa en bloques de 512 bits.

3.3.2 Envió de mensaje usando la función HASH

Al enviar un mensaje junto con su hash, es posible garantizar la integridad de dicho mensaje, es decir, el destinatario puede estar seguro de que el mensaje no ha sido alterado (intencionalmente o por casualidad) durante la comunicación.

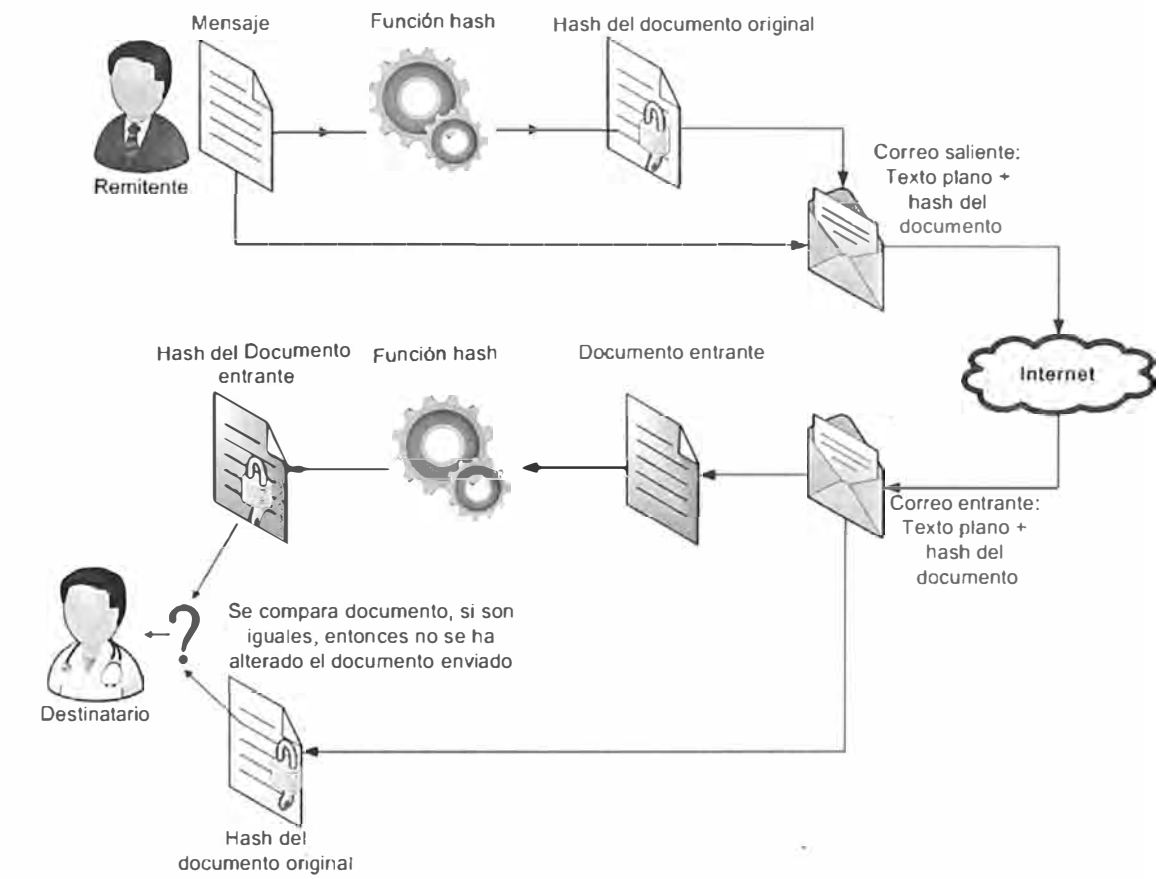


Fig. 3.5: Envío de mensaje utilizando funcion hash

Cuando un destinatario recibe un mensaje simplemente debe calcular el hash del mensaje recibido y compararlo con el hash que acompaña el documento. Si se falsificara el mensaje (o el hash) durante la comunicación, las dos huellas digitales de los documentos no coincidirían (ver Fig. 3.5).

Al utilizar una función hash se puede verificar que la huella digital del documento corresponde al mensaje recibido, pero no se puede probar que el mensaje haya sido enviado por la persona que afirma ser el remitente, para solucionar este problema se debe realizar el proceso de firma digital del hash del documento.

3.4 Certificado digital

El Certificado Digital es un documento digital (ver Fig.3.6) mediante el cual una Entidad Certificadora garantiza la relación entre la identidad de una persona natural o persona jurídica y su clave pública y clave privada.

Fig. 3.6: Informacion de certificado digital

La Entidad de Certificación es una organización confiable que emite o revoca certificados digitales, mediante la validación y autentificación de dichas solicitudes.

La clave pública permite cifrar el mensaje a enviar (puede ser compartida con cualquier persona), mientras que la clave privada permite descifrarlo (solo tiene acceso el propietario del certificado, la misma puede ser almacenada en una tarjeta inteligente, token criptográfico, etc. (ver Fig. 3.7).

Fig.3.7: Dispositivos de almacenamiento

Un certificado digital permite identificarse en Internet así como intercambiar información con otras personas, con la garantía de que sólo quien posee la llave privada puede tener acceso a dicha información.

Los certificados digitales son utilizados para aumentar la seguridad de las transacciones en Internet y ayudan a disminuir los fraudes virtuales por suplantaciones de identidad (tanto de personas naturales como personas jurídicas).

Los certificados digitales permiten verificar que la información que se envía es auténtica, es decir que el remitente sea realmente quien dice ser.

Así pues los certificados digitales, proporcionan un mecanismo para verificar la autenticidad de documentos obtenidos a través de la red, como por ejemplo el envío de correo encriptado, control de acceso a recursos, la validación oficial de documentos electrónicos, etc.

3.4.1 Obtención del certificado digital

El certificado digital se obtiene cuando el solicitante del certificado digital se apersona a las oficinas de una ER y solicita la expedición del mismo. La ER se encarga de validar la identidad del solicitante y en caso positivo, autoriza la expedición del mismo a la EC (ver gráfico Nº 3.8), la EC es la encargada de generar el certificado digital con los datos del solicitante.

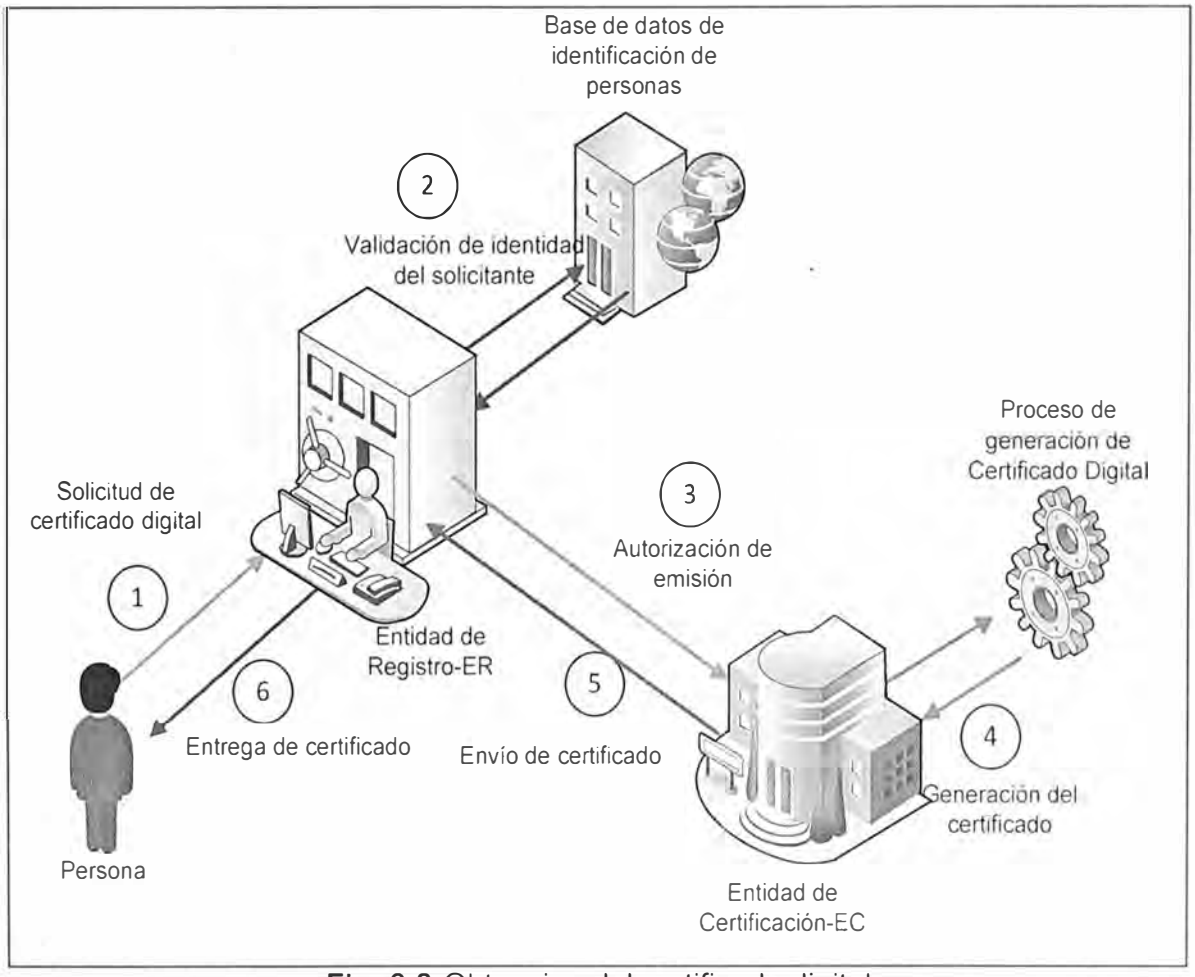


Fig. 3.8: Obtencion del certificado digital

3.5 Clave pública y clave privada

La clave pública y clave privada son una parte muy importante de los procesos de certificación digital (firma digital, cifrado, sello de tiempo, autenticación, etc.), ya que la seguridad de estos procesos de basa en el fundamento matemático que soporta a la clave pública y la clave privada (factorización de números primos).

3.5.1 Características de la clave pública y clave privada

Las características de estas claves son:

- La clave pública es conocida por las demás personas(esta clave esta publicada en un repositorio previamente establecido y
- la clave privada permanece bajo el exclusivo control de su propietario.

3.5.2 Fundamento matemático del par de claves

El concepto matemático detrás de la clave pública y clave privada son las funciones unidireccionales (aquella cuya computación es fácil en un sentido, mientras que el proceso inverso resulta extremadamente difícil), específicamente la factorización de números primos. El funcionamiento se describe a continuación, la clave pública contiene un primer factor primo grande, y el algoritmo de cifrado usa la clave pública para cifrar el mensaje. El algoritmo para descifrar el mensaje requiere el conocimiento del segundo factor (clave privada), para que el descifrado sea posible, si es que no se tiene el segundo factor es extremadamente difícil (casi imposible) obtener a partir de la clave pública (si es que tiene un tamaño de clave es adecuado) la clave privada. Como se observa, toda la seguridad descansa en el tamaño de la clave. Por lo tanto el tamaño de la clave es una medida del seguridad del sistema. En un ataque de fuerza bruta sobre un cifrado de clave pública con un tamaño de clave de 256 bits o menos, puede ser factorizado en pocas horas con un computador personal, usando software libre, si la clave tiene 512 bits o menos, puede ser factorizado por varios cientos de computadoras como en 1999[6].

Actualmente es recomendado que el tamaño de la clave sea como mínimo de 2048 bits de longitud.

3.6 Firma digital

Actualmente la validación de la mayoría de documentos legales, financieros y otros tipos se determina por la presencia o ausencia de una firma manuscrita autorizada. Para que los documentos electrónicos reemplacen el transporte físico de papel y tinta, debe encontrarse un método o mecanismo con el mismo nivel de seguridad de la firma manuscrita.

El problema de reemplazar las firmas manuscritas en el internet es difícil. Básicamente, lo que se requiere es un sistema mediante el cual una parte pueda enviar un mensaje "firmado" a otra parte de modo que:

- El receptor pueda verificar la identidad proclamada del transmisor.
- El transmisor no pueda repudiar después el contenido del mensaje.
- El receptor no haya podido confeccionar el mensaje él mismo.

Estas condiciones solamente son cumplidas con la firma digital, para comprender el concepto de firma digital, imaginemos que se dispone de un documento a enviar, entonces mediante una función hash calculamos el hash del documento y luego realiza el proceso de cifrado utilizando la clave privada del remitente. Ahora trasmitimos el mensaje firmado digitalmente (mensaje original y el hash cifrado, ver Fig.3.9). El destinatario, recepciona el mensaje, descifra el hash con la clave pública del emisor y calcula el hash del mensaje recibido y obtiene la misma secuencia de caracteres (ver Fig.3.10), entonces se puede concluir:

- La integridad del mensaje no has sido alterada, dado que el hash calculado es igual al hash descifrado.
- El origen del mensaje es correcto, ya que el al utilizar la clave pública del remitente para obtener que hash descifrado y ser igual al hash calculado, se comprueba que existe una vinculación entre el mensaje y la clave privada del remitente.

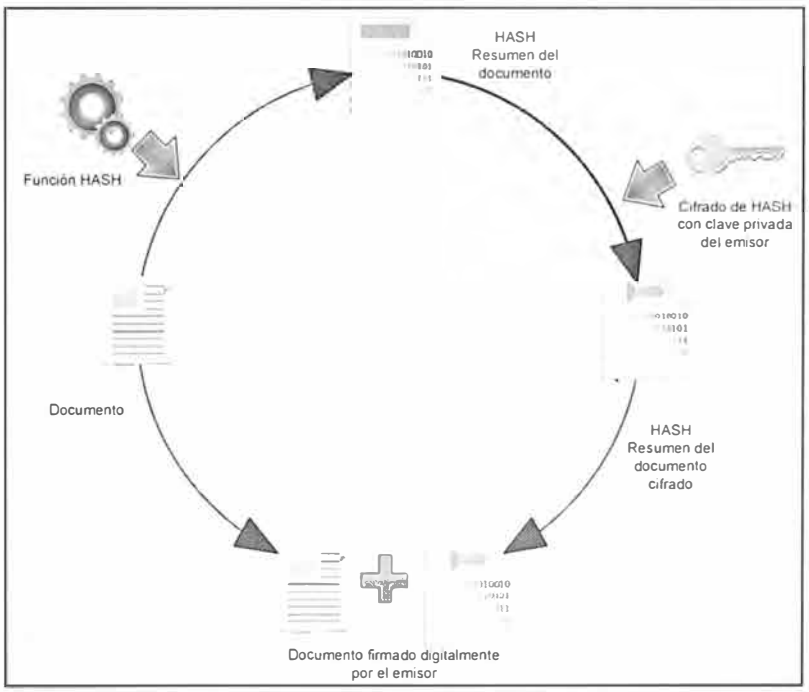


Fig. 3.9: Proceso de firma digital

La ventaja de cifrar sólo el hash y no todo el documento salta a la vista: eficiencia. Es mucho más sencillo cifrar un resumen del mensaje (hash) y no todo el documento. Producir el hash a partir del mensaje de entrada requiere muchos menos recursos computacionales y por tanto menos tiempo de cómputo.

Un mensaje al que se ha agregado el hash cifrado se dice que está *Firmado Digitalmente*. Las firmas digitales no sirven solo para autenticar mensajes si no que pueden ser utilizados para probar la autenticidad de cualquier documento electrónico.

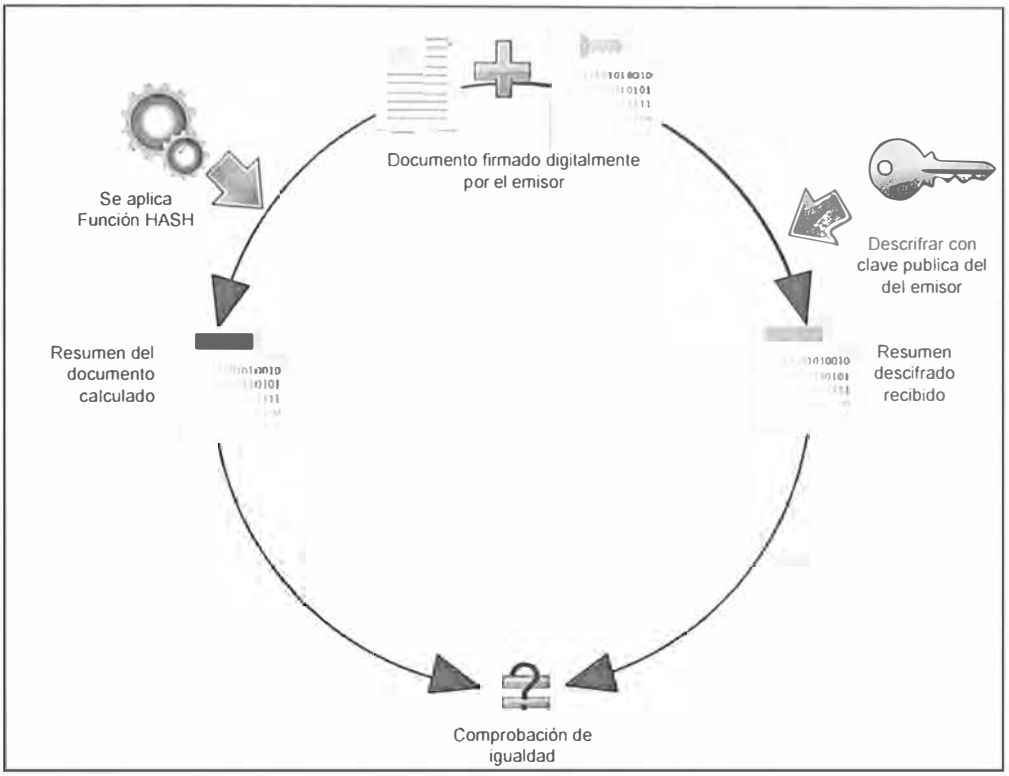


Fig. 3.10: Proceso de comprobacion de firma digital

Una firma digital permite verificar el autor del documento,. Adicionalmente la firma digital puede ser verificable por terceros, ya que el proceso de firma digital no modifica ni hace ilegible el documento original a diferencia del proceso de cifrado, tal como se puede ver en la Fig. 3.11, donde la imagen de la izquierda el el documento sin firma digital y la imagen de la derecha es el docuemto luego del proceso de firma digital.

Fig 3.11: Documento antes y despues del proceso de firma digital

Un algoritmo específicamente para firma digital es DSA, Algoritmo de Firma digital en español (DSA Digital Signature Algorithm en inglés) es un estándar del Gobierno Federal de los Estados Unidos de América o FIPS para firmas digitales. Fue un Algoritmo propuesto por el Instituto Nacional de Normas y Tecnología de los Estados Unidos, especificado en el FIPS 186. Una desventaja de este algoritmo es que requiere mucho más tiempo de cómputo que RSA.

3.6.1 Estándares de firma digital

Se indican a continuación algunos de los estándares usados en el proceso de firma digital:

- X.509 V3 Formatos Estándar para Certificados de Claves Públicas
- Estándar Asimétrico RSA ANSI x3.09 Parte 1
- FIPS 180-2 Algoritmo de Hashing SHA-1, SHA-256
- FIPS 186 Estándar de Firma Digital (DSA)
- PKCS#1 Estándar de Criptografía RSA: define la criptografía RSA
- PKCS#11Estándar de Interfaz de Token Criptográfico
- PKCS#12 Sintaxis de Intercambio de Información Personal

3.7 Cifrado de datos

El cifrado es básicamente transformar datos en alguna forma que no sea legible sin el conocimiento de la clave o algoritmo adecuado. El propósito de esta es mantener oculta la información que consideramos privada a cualquier persona o sistema que no tenga permitido verla, esto garantiza el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y asegura que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado no haya sido modificado en su tránsito.

3.7.1 Tipos de cifrado

Los tipos de cifrado son:

a. Cifrado simétrico

El emisor cifra el mensaje con una clave, y esa misma clave deberá ser la utilizada para descifrarlo (ver Fig Nº 3.12). Estos algoritmos son rápidos y permiten cifrar y descifrar eficientemente con claves relativamente grandes. La seguridad de este tipo de criptografía radica principalmente en mantener en secreto la clave y no se preocupa necesariamente por el algoritmo de cifrado, es decir, que no es de mucha ayuda conocer el algoritmo que se utilizó. Uno de los principales inconvenientes con este tipo de sistema es que no está ligado a su seguridad, sino al intercambio de claves.

Fig. 3.12: Proceso del cifrado simetrico

El canal utilizado para el intercambio de la clave debe ser lo suficientemente seguro. Una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad.

Otro problema es el número de claves que se necesitan. Si tenemos un número n de personas que necesitan comunicarse entre sí, se necesitan n/2 claves para cada pareja de personas que tengan que comunicarse de modo privado. Esto puede funcionar con un grupo reducido de personas, pero sería imposible llevarlo a cabo con grupos más grandes.

Algunos algoritmos de cifrado simétrico son:

- **Blowfish:** Es uno de los más efectivos hasta este momento, está basado en las funciones de Feistel, Blowfish usa bloques de 64 bits y claves que van desde los 32 bits hasta 448 bits. Dada su complejidad, no es apto para entornos donde los recursos de memoria de procesamiento de datos sea limitada.
- **IDEA:** La primera versión de IDEA (Algoritmo Internacional de Cifrado de Datos en español) fue dada conocer en 1990 bajo el nombre de Proposed Encyption Standard (PES), dos años después, luego de haber sido reforzado para resistir nuevos tipos de ataque cambio su nombre a IDEA.IDEA utiliza una clave de 128 bits, lo que por el momento lo hace inmune a los ataques de fuerza bruta así como al criptoanálisis diferencial para su desencriptado. La estructura básica consiste en la alteración de bloques de entrada de texto normal de 64 bits en una secuencia de iteraciones parametrizadas para producir bloques de salida de texto cifrado de 64 bits.

b. Cifrado asimétrico

Para este tipo de cifrado se utiliza la clave pública y privada, estas son generadas por la entidad de certificación(EC) a solicitud de la Entidad de Registro (ER). El procedimiento es el siguiente, el emisor cifra el mensaje con la clave pública del destinatario, que es la que conoce. Sin embargo para descifrarlo hace falta la clave privada del destinatario, que sólo el conoce, ya que es privada. Con esto se garantiza confidencialidad, cualquiera podría cifrar, pero sólo quien tenga la clave privada podrá descifrar (ver Fig. 3.13).

Fig. 3.13: Proceso del cifrado asimetrico

El funcionamiento de estos algoritmos, está basado en factorización de números primos. Este algoritmo garantiza la seguridad de la clave privada, ya que sólo la tiene el receptor.

Las principales ventajas de este tipo de criptografía es que la clave secreta ya no tiene que transmitirse entre los interlocutores y tampoco es necesario tener claves

diferentes para cada pareja de interlocutores, es suficiente con que cada usuario tenga su clave pública y su clave privada.

El principal problema de este procedimiento es el tiempo requerido para descifrar y el tamaño de los archivos cifrados es mayor en comparación con el cifrado simétrico,

El método de cifrado de datos conocido como algoritmo RSA, por los nombres de sus inventores (Rivest, Shamir y Adleman) es uno de los más extendidohoy en día tanto cifrar como para firmar digitalmente, por lo que se usa para la transmisión segura de datos a través de canales inseguros. Este algoritmo es reversible, es decir, además de permitir cifrar con la clave pública y descifrar con la privada, permite cifrar con la clave privada y descifrar con la clave pública.

3.7.2 Estándares de cifrado

Se indican a continuación algunos de los estándares usados en el proceso de cifrado:

- FIPS 46 Estándar de Cifrado de Datos (DES)
- FIPS 197 Estándar de Cifrado Avanzado (AES)
- RFC 1231 Algoritmo de Hashing MD5

3.8 Sello de tiempo

El sellado de tiempo es un mecanismo para probar que un conjunto de datos existió en un momento dado y que ninguno de estos datos ha sido modificado desde entonces(ver Fig. 3.14).

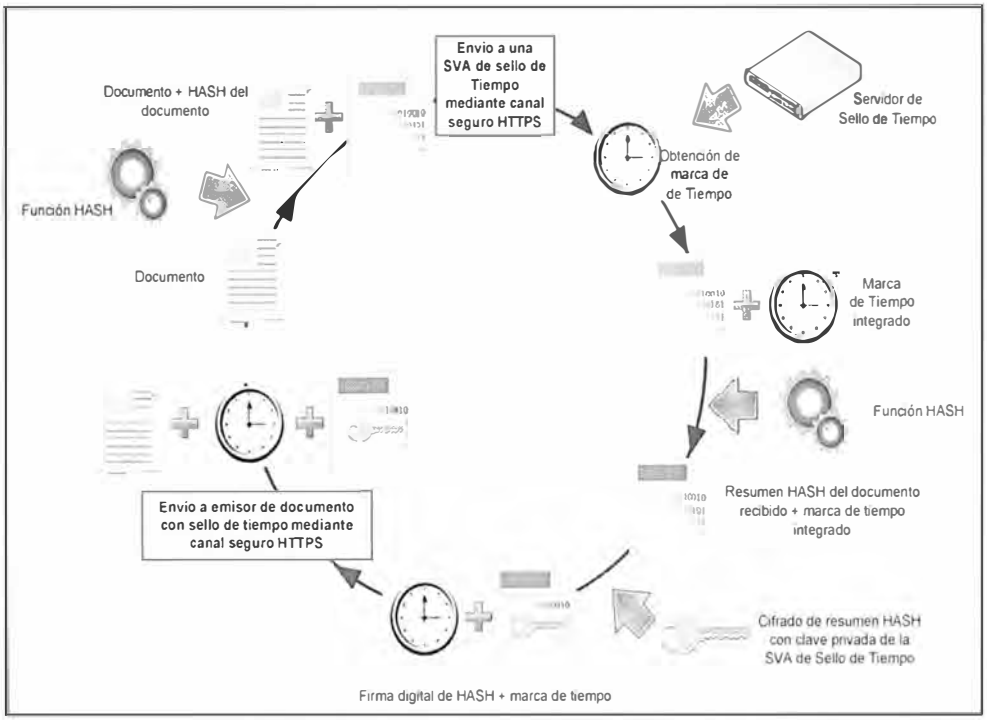


Fig. 3.14: Proceso de funcionamiento de sello de tiempo

El sellado de tiempo proporciona un valor añadido a la utilización de firma digital ya que ésta por sí sola no proporciona ninguna información acerca del momento de creación de la firma, y en el caso de que el firmante la incluyese, ésta habría sido

proporcionada por una de las partes, lo cual generaría una duda razonable sobre la veracidad de la misma por lo que es necesario que el servicio sello de tiempo sea proporcionada por una tercera parte de confianza, en el caso peruano este tercero de confianza es denominado SVA de sello de tiempo.

3.8.1 Caracteristicas del proceso

A través de la interfaz de validación, pueden validarse sellos de tiempo emitidos previamente con la finalidad de saber si en esa fecha dada el sello de tiempo era válido (ver Fig. 3.15), el mecanismo de validación descifra con la clave publica de la SVA de sello de tiempo, luego aplica la funcion hash y compara este documento con el que resulta de aplicar la funcion hash al documento recepcionado, si la verificacion tanto de la autenticidad del cifrado de la SVA, asi como de la marca de tiempo, es positiva, entonces se puede concluir que el documento en el instante del sello de tiempo es autentico, verdadero.

Un mecanismo adicional al sello de tiempo es el de la interfaz de resellado, con el cual se puede volver a sellar, sellos previamente emitidos, con lo se puede obtener un cadena de confianza de sellos de tiempo.

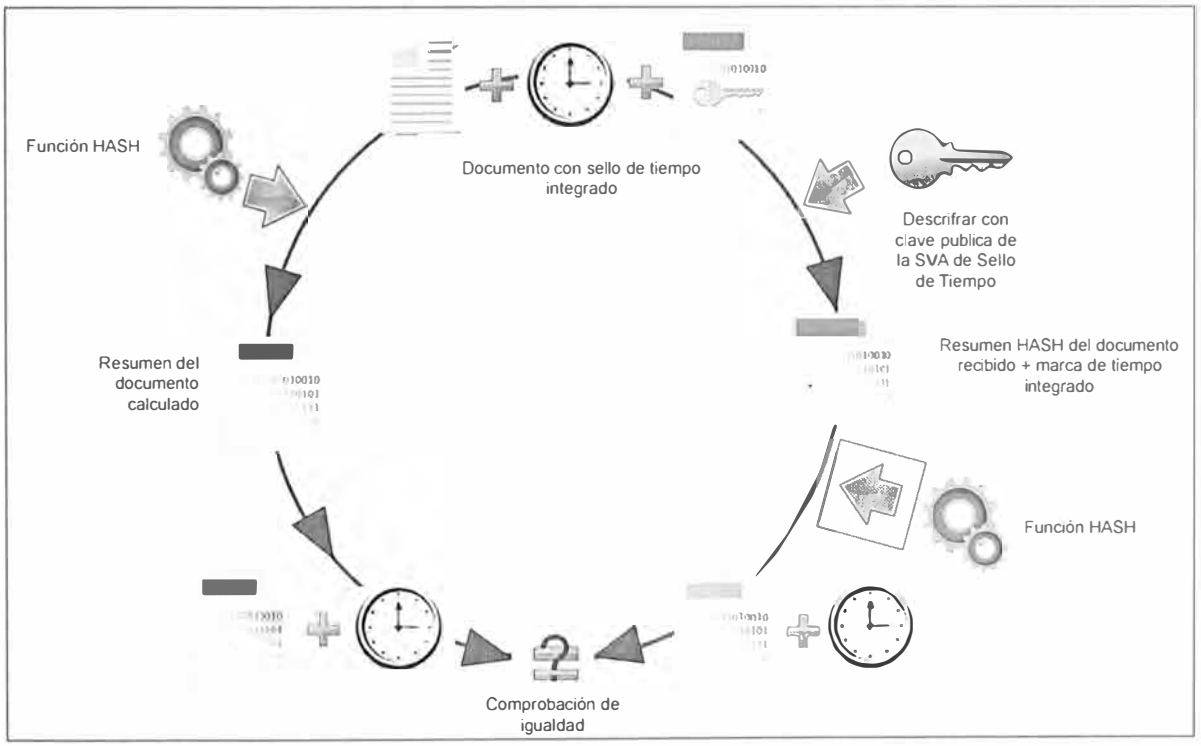


Fig. 3.15 Proceso de verificación de sello de tiempo

3.8.2 Estándares de sello de tiempo

Se indican a continuación algunos de los estándares usados en el proceso de sello de tiempo:

- RFC 3161 "Internet X.509 Public Key Infrastructure Time StampProtocols ", estándar definido por la Internet EngineeringTaskForce (IETF) para el protocolo Time Stamp.
- IETF RFC 3628 Policy Requirements for Time-Stamping Authorities (TSAs).

- ETSI TS 102 023 Policy requirements for time-stamping Authorities.
- XML Timestamping Profile of the Digital Signature Services (DSS) ver. 1.0.
- ETSI TS 101 861 Time stamping profile.

3.8.3 NTP

NTP o Network Time Protocol en inglés, fue diseñado para sincronizar el reloj de la máquina cliente con el reloj de los servidores NTP. Pero el NTP no es sólo el protocolo. La implementación del NTP requiere clientes y aplicaciones de servidor separados.

NTP ha sido portado a prácticamente todas las plataformas de computadoras, desde supercomputadoras hasta las modestas computadoras personales (PC). Así un reloj de computadora en Lima, puede estar en sincronía con un reloj de computadora en la India.

3.8.4 Desarrollo del protocolo NTP

Fue desarrollado en la Universidad de Delaware por el Dr. David Mills[7], las especificaciones para la versión 3 fueron liberados en1992 (RFC 1305), la versión 4 es la versión actual[8], algunas de las nuevas características incluyen la autenticación por medios criptográficos.

3.8.5 Funcionamiento del protocolo NTP

El Network Time Protocol (NTP) se usa para sincronizar la hora de una computadora cliente o servidor a la hora de otro máquina servidor o a una fuente de referencia, a través de un receptor radio o una conexión vía satélite (ver Fig. 3.16.)

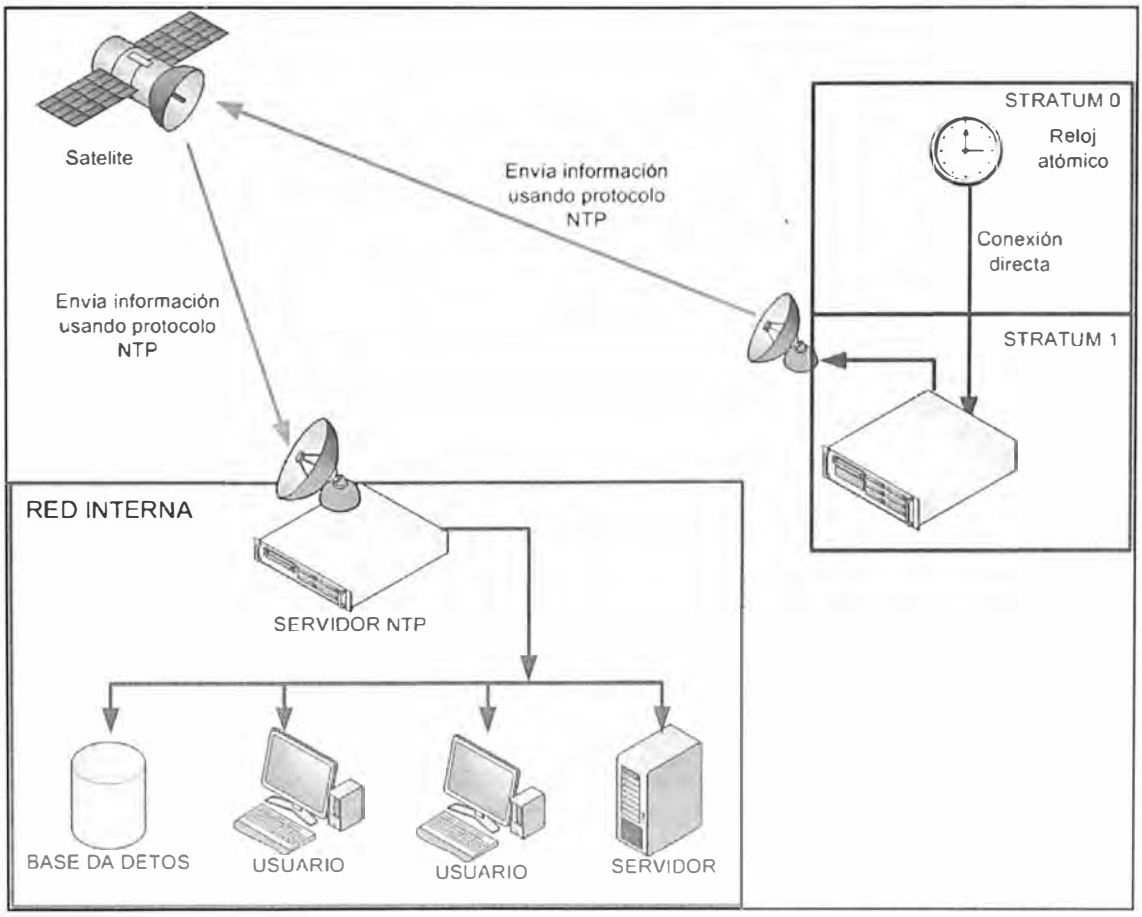


Fig. 3.16: Proceso de funcionamiento de NTP

Típicamente, las configuraciones de NTP utilizan tanto servidores como caminos redundantes, proporcionando así exactitud y fiabilidad. Inclusive algunas configuraciones permiten autenticación para prevenir ataques accidentales o maliciosos al protocolo.

3.8.6 Exactitud del protocolo NTP

Depende de cuántos saltos ocurran entre el cliente y el servidor y otros factores de red que induzcan a la latencia. En una Red de Área Amplia (Wide Area Network, WAN, por sus siglas en inglés) de 10 a 100 milisegundos es lo normal. Dentro de una Red de Área Local (Local Area Network, LAN, por sus siglas en inglés) de 0.5 a 2 milisegundos.

3.8.7 Servidor NTP

Se entiende como servidor NTP a un dispositivo de red que obtiene la hora de una fuente alterna (Niveles Stratum), mantiene la hora en su reloj interno y suministra la hora a una red conectada utilizando el protocolo NTP.

3.8.8 Niveles stratum

Clasifica los servidores en niveles (estratos), indicando de esta forma cuál es la distancia de este servidor a un reloj de referencia. El nivel 1 indica un servidor directamente conectado a un reloj de referencia, mientras que el mayor nivel (stratum 16[9]) muchas veces indica que el reloj se encuentra inoperante o inaccesible. De modo general, un servidor de stratum "n" se encuentra a (n-1) saltos del stratum 1 de la jerarquía NTP a la cual pertenece (ver Fig. 3.17).

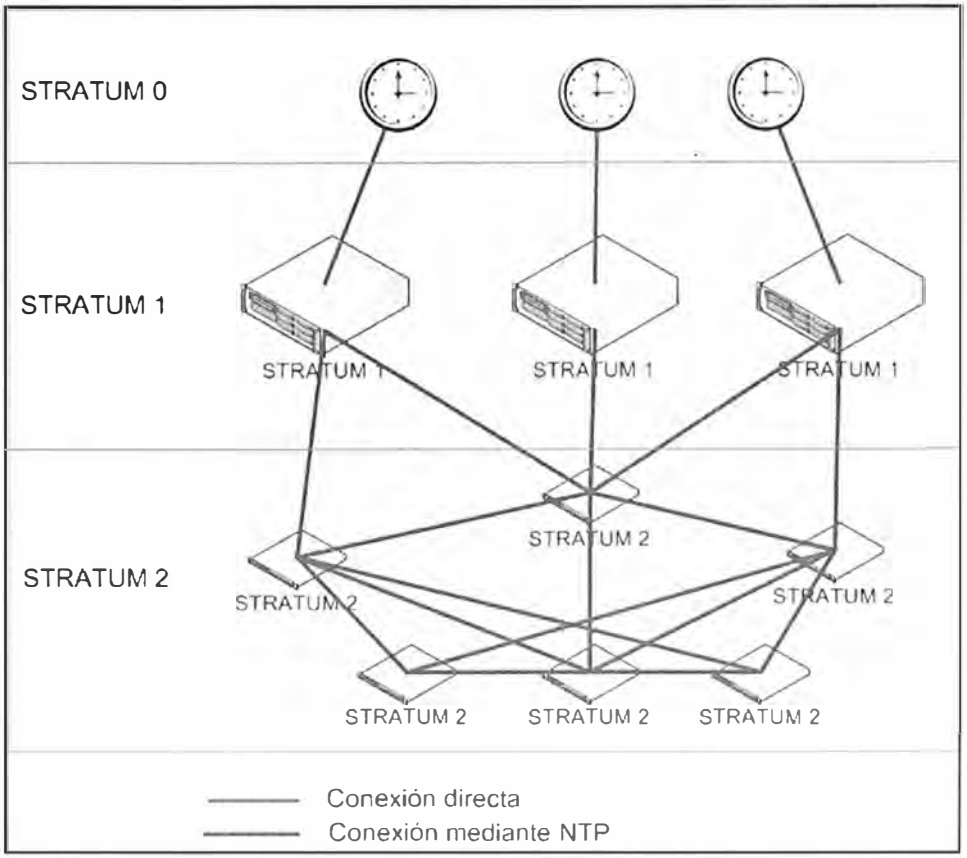


Fig. 3.17: Jerarquía NTP

3.8.9 Configuraciones NTP

El protocolo NTP puede trabajar bajo diferentes configuraciones, algunas de las cuales son [11]:

- Modo simétrico
- Modo broadcast
- Multicast IP

1. Modo simétrico, el cual permite a cada uno de los dos servidores sincronizarse con otro, para proporcionarse copias de seguridad mutuamente (ver Fig. 3.18).

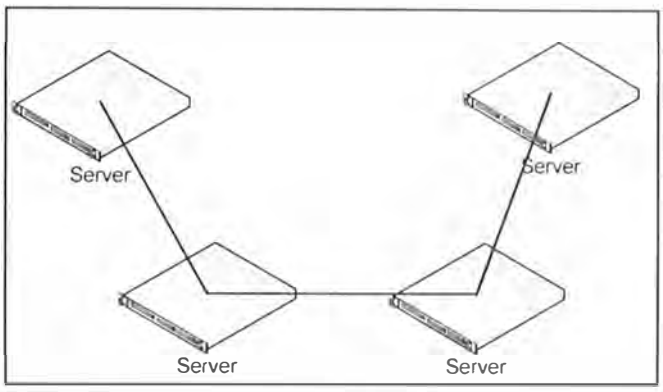


Fig. 3.18: NTP modo simétrico

2. Modo broadcast, por el cual muchos clientes pueden sincronizarse con uno o varios servidores, reduciendo el tráfico en la red cuando están involucrados un gran número de clientes (ver Fig. 3.19).

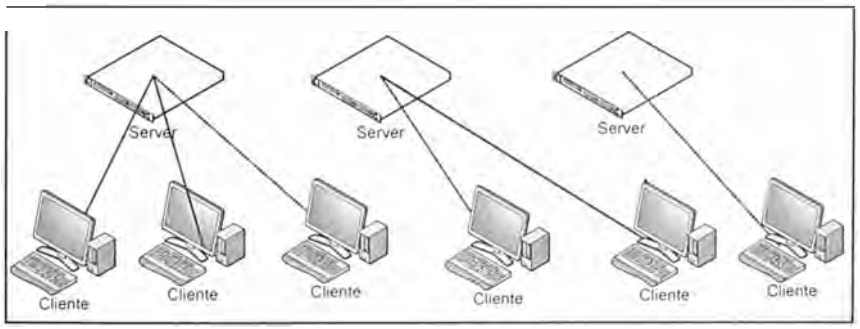


Fig. 3.19: NTP modo broadcast

3. Multicast IP, también puede ser usado cuando la subred se abarca múltiples redes de trabajo (ver Fig.Nº 3.20).

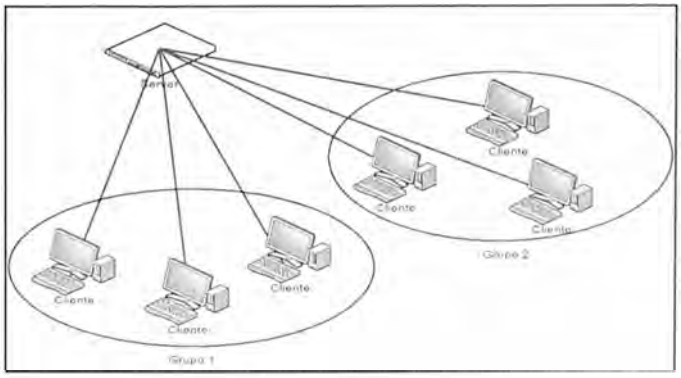


Fig. 3.20: NTP modo multicast

3.8.10 Estructura del protocolo NTP

En la TABLA Nº 3.2, se muestra la Cabecera del protocolo NTP, conforme a la versión NTP v3 y NTP v4.

TABLA Nº 3.2: Estructura del protocolo NTP

ESTRUCTURA	LI	VN	Modo	Stratus	Registro	Precisión
	Demora de raíz					
	Dispersión de la raíz					
	Identificador de referencia					
	Sello de Tiempo de referencia (64)					
	Sello de Tiempo de referencia (64)					
	Sello de tiempo de origen (64)					
	Sello de tiempo recibido (64)					
	Sello de tiempo transmitido (64)					
	Campo 1 (opcional)					
	Campo 2 (opcional)					
AUTENTICADOR (OPCIONAL)	Algoritmo identificador					
	Resumen de mensaje (128)					

Leyenda:

NTP v3 y v4
NTP v4 solamente
Solo para autenticación

3.8.11 Variables del protocolo NTP

A continuación se muestras las variables del protocolo NTP[7].

- **Indicador de advertencia-LI (Leap Indicator en inglés)**

Código de 2 bits que sirve para indicar que al último minuto del presente día se le añadirá/quitará un segundo.

TABLA Nº 3.3: Variable Indicador de Advertencia

LI	Valor	Significado
0	0	sin modificación
1	1	el último minuto tiene 61 segundos
10	2	el último minuto tiene 59 segundos
11	3	condición de alarma (reloj no sincronizado)

- **Numero de versión-VN (Versión Number en inglés)**

Entero de 3 bits que indica el número de versión. La versión 3, indica la versión 3 (sólo IPv4) y la 4 para la versión 4 (IPv4, IPv6 y OSI). Si es necesario distinguir entre IPv4, IPv6 y OSI, se debe examinar el contexto encapsulado.

Tabla Nº 3.4: Variable Numero de versión

VN	Significado
3	NTP v3 (sólo IPv4)
4	NTP v4 (IPv4, IPv6 y OSI)

- **Modo (Mode en inglés)**

Entero de tres bits que sirve para indicar el modo, definidos de la siguiente manera:

Tabla Nº 3.5: Variable Modo

Modo	Significado
0	reservado
1	simétrico activo
2	simétrico pasivo
3	Cliente
4	Servidor
5	broadcast
6	reservado para mensajes de control de NTP
7	reservado

- **Stratum**

Es un entero sin signo de 8 bits que indica el nivel (stratum) del servidor local, los valores definidos son los siguientes:

Tabla Nº 3.6: Variable Stratum

Stratum	Significado
0	no especificado o no disponible
1	referencia primaria (ej., radio clock)
2 -15	referencia secundaria (vía NTP o SNTP)
16	Inaccesible

- **Registro**

Es un entero de 8 bits con signo que indica el intervalo máximo de tiempo entre dos mensajes sucesivos, expresado en segundo y como la potencia de 2 más cercana. La mayoría de las aplicaciones usan el rango que va desde 6 bits 10 bits.

- **Precisión**

Es un entero con signo que indica la precisión del reloj local expresado en segundo a la potencia de 2 más cercana.

3.8.12 Estándares usados

Se indican a continuación algunos de los estándares usados para el uso del protocolo:

RFC 5905: Network Time Protocol Version 4: Protocol and Algorithms Specification

RFC 5906: Network Time Protocol Version 4: Autokey Specification

- RFC 5907: Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4)

RFC 5908: Network Time Protocol (NTP) Server Option for DHCPv6

3.8.13 Seguridad

NTP se basa en el protocolo UDP y utiliza el puerto UDP 123, ccomo tal, es altamente susceptible a lafalsificación de direcciones IP, una solución a este problema es el bloqueo de este puerto en el firewall para mantener la seguridad dentro del perímetro de la red, pero esto impide que un cliente obtenga datos de tiempo de un servidor NTP.

Para mantener los niveles de seguridad y disponibilidad del servicio es necesario que el servidor NTP esté instalado dentro de la DMZ y que adquiera el tiempo vía GPS.

La seguridad se maximiza cuando el servidor de tiempo está instalado después del firewall de red. El servidor NTP adquiere el tiempo vía conexión GPS, por medio de una antena, sin amenaza para la seguridad de la red. A continuación, distribuye el tiempo a los clientes a lo largo de la red con firewall.

Para mejorar la seguridad de las amenazas contenidas en el firewall, el servidor NTP debe utilizar técnicas de control de acceso y autenticación para restringir el acceso al servicio NTP. Sólo paquetes NTP autenticados deben ser aceptados [11].

El servidor NTP debe aceptar paquetes de fuentes aprobadas. Para comunicar con el servidor NTP para el estado y el control es mejor utilizar un protocolo de seguridad, tal como Secure Shell (SSH) y/o SNMP v3 (SNMP cifrada). (SNMP v1 y v2c no son seguros). Además, la seguridad es aún mayor si los protocolos tales como FTP, Telnet, se desactivan.

3.8.14 Consumo de recursos

El protocolo NTP requiere poco consumo de recursos, lo que le permite ser desplegado en servidores de alojamiento de otros servicios, incluso si los servidores tienen una alta carga de trabajo. Los requisitos de ancho de banda son también mínimos, ya que los paquetes NTP solo consumen 60 bytes de longitud. Un cliente/servidor NTP de transacciones requiere de 2 paquetes por transacción. Las transacciones se realizan aproximadamente una vez por minuto, cambiando gradualmente a una vez cada 15 minutos.

3.8.15 Software de cliente NTP

Además de agregar un servidor NTP a la red, también se requiere que el software de cliente NTP debe estar instalado en cada una de las estaciones de trabajo los servidores que se conectarán con el servidor de tiempo. En la mayoría de los casos el software

cliente ya está residente en el sistema operativo de la estación de trabajo, servidor, router o firewall. En otros casos, hay que descargar el cliente.

3.9 Satélites

Un satélite actúa básicamente como un repetidor situado en el espacio: recibe las señales enviadas desde la estación terrestre y las reenvía a otro satélite o de vuelta a los receptores terrestres (ver Fig. 3.21).

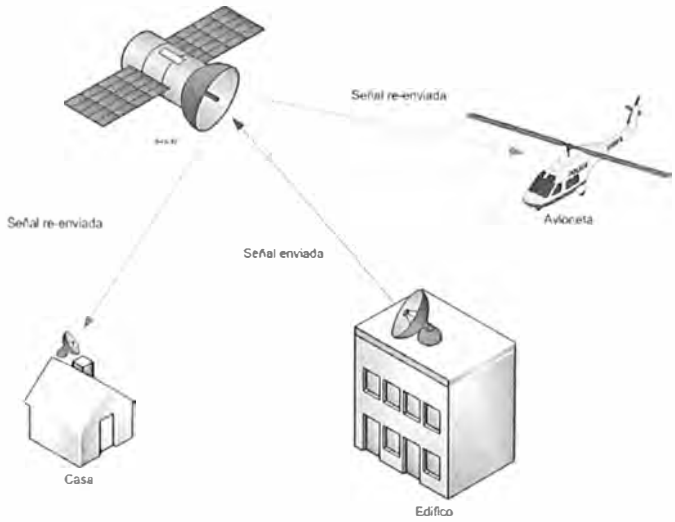


Fig.3.21: Operación de un satélite

3.9.1 Tipos de satélite

En realidad hay dos tipos de satélites de comunicaciones:

- Satélites pasivos. Se limitan a reflejar la señal recibida sin llevar a cabo ninguna otra tarea.
- Satélites activos. Amplifican las señales que reciben antes de reenviarlas hacia la Tierra.

3.9.2 Orbitas de satélites

Los tipos de satélites según sus órbitas se indican en la tabla siguiente:

TABLA Nº 3.7 Orbitas de satélites

Orbita	Altura orbital	Aplicaciones
LEO	~<1500 km	Experimentación científica, comunicaciones, lanzamientos de satélites GEO o misiones interplanetarias Servicios: comunicaciones, vigilancia, meteorología, etc.
SSO		Para satélites de observación, siempre se toman los datos en las mismas condiciones
MEO	10000 – 30000km	Navegación: Constelaciones GPS, Glonass, Galileo
GEO	~36000 km	Radiodifusión, comunicación, meteorología, redes VSAT, etc.
HEO	~>20000 km	Comunicaciones, observación espacial.

3.10Balanceadores de carga

Un balanceador de carga es un dispositivo hardware o software (ver Fig. 3.22 y Fig. 3.23), que se pone al frente de un conjunto de servidores que atienden una petición de servicio (aplicación, acceso, etc.) y, asigna o balancea las solicitudes que llegan de los clientes a los servidores usando algún algoritmo (desde un simple round-robin hasta algoritmos más sofisticados).

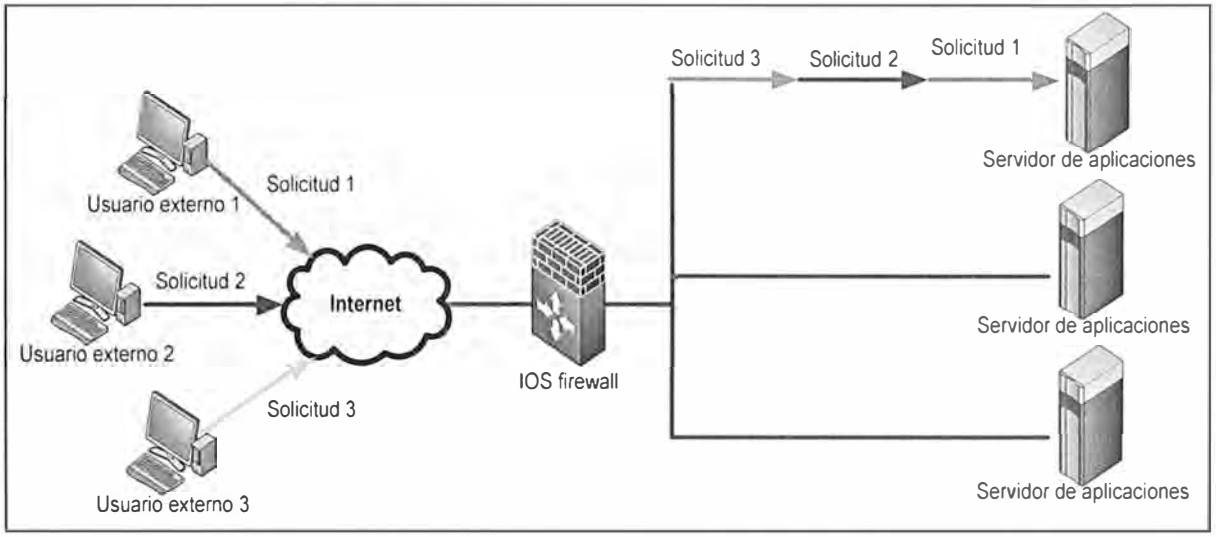


Fig. 3.22: Dispositivo balanceador de carga por software

El balance de carga se mantiene gracias a un algoritmo que divide de la manera más equitativa posible el trabajo, para evitar los así denominados cuellos de botella.

Esto íntimamente ligado a los sistemas de multiprocesamiento, o que hacen uso de más de una unidad de procesamiento.

Un balanceador de carga soluciona uno de los principales problemas de los sitios web en Internet que es cómo gestionar las solicitudes de un gran número de usuarios. Se trata de un problema de escalabilidad que surge con el continuo crecimiento del número de usuarios activos en el sistema.

Hay balanceadores de carga tipo round-robin (uno a uno) y por pesos, los cuales son capaces de saber cuál de los nodos está más libre y lanzarle la petición (ver Fig. 3.23).

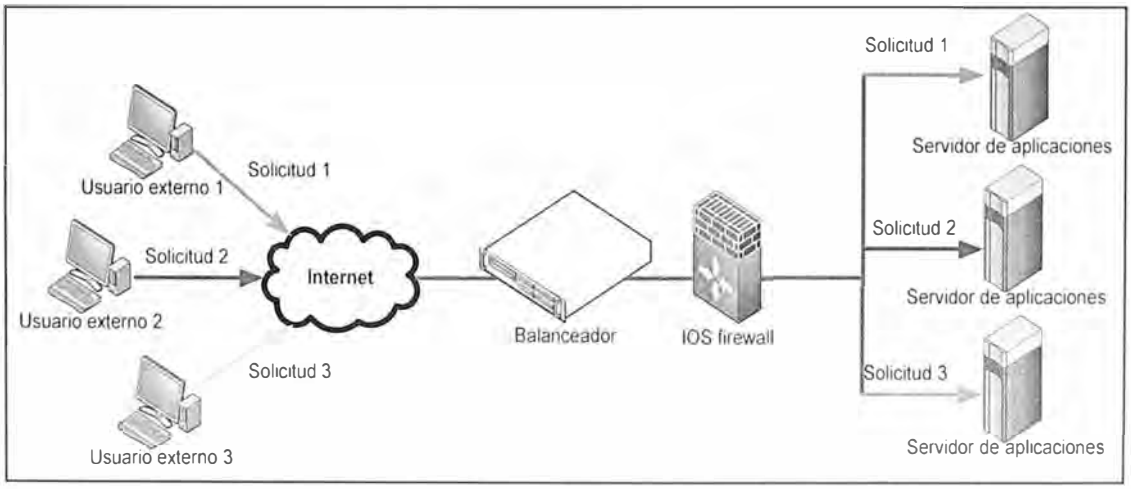


Fig. 3.23: Dispositivo hardware balanceador de carga

3.11 Firewall

Un firewall (cortafuego) es dispositivo que protege los equipos conectados en red contra intrusiones hostiles intencionales o no intencionales que pueden comprometer la confidencialidad o dañar los datos o causar una denegación de servicio.

El firewall se encuentra en el punto de unión o puente entre las dos redes, por lo general una red privada y una red pública como Internet.

Los firewall puede ser de dos tipos:

- hardware
- aplicativo de software que se ejecuta en una computadora.

En cualquier caso, se debe tener al menos dos interfaces de red:

- Una para la red que se pretende proteger,
- y una para la red que está en conexión abierta.

Para que se entienda mejor el funcionamiento del firewall ver la Fig. 3.24.

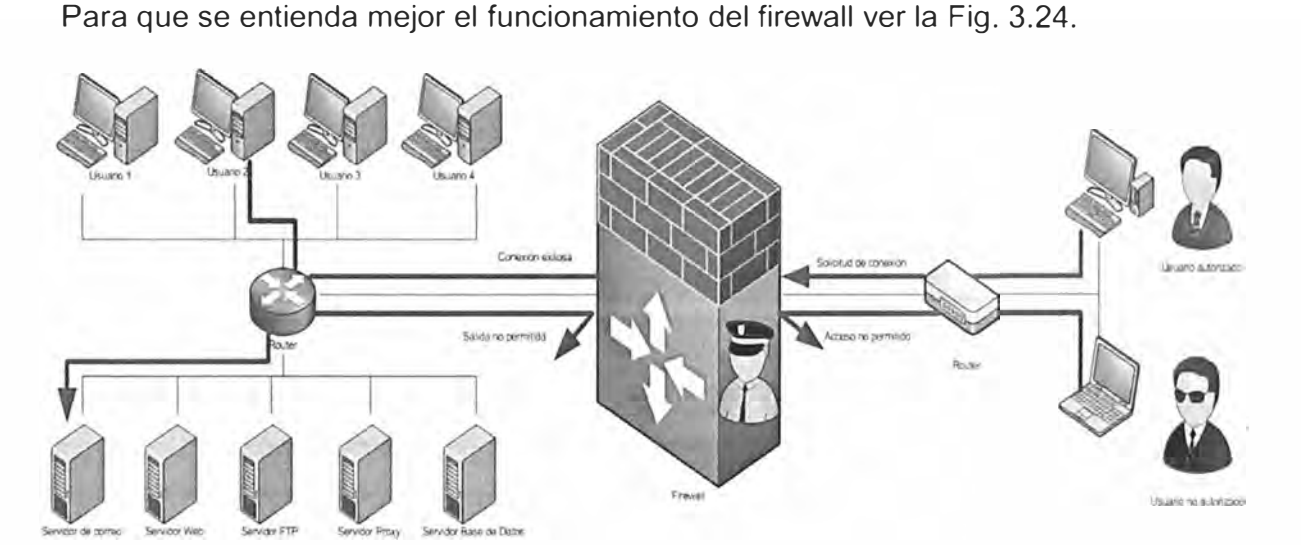


Fig. 3.24: Operación de dispositivo firewall

3.11.1 Modo de funcionamiento del firewall

El término firewall viene del hecho de que mediante la segmentación de la red en diferentes subredes físicas, limita el daño que podría extenderse a partir de una subred a otra igual. De manera muy concreta un firewall es un packetfilter (filtrador de paquetes) entre los dispositivos conectados a esta, este filtrado de paquetes puede ser en varios niveles del modelo OSI.

El firewall define un conjunto de reglas y políticas para filtrar los paquetes que pasan por este dispositivo, de acuerdo a este conjunto de reglas y políticas establecidas se decida si se autoriza un acceso o salida de la red.

Parecería entonces, que los firewalls funcionando a un nivel superior de la capa debería tener características superiores en todos los aspectos. Esto no es necesariamente cierto. Cuanto más baja es la capa del paquete interceptado, es más seguro el firewalls.

3.11.2 Tipos de firewalls

Se clasifican en dos grandes grupos:

a. Firewall por software

Un firewall por software es una aplicación y el funcionamiento del mismo está basado en un conjunto de reglas, pero no tiene la capacidad, ni los recursos necesarios para procesar a gran velocidad las transacciones de datos, su uso frecuentemente está orientado a usuarios finales (ver Fig. 3.25), el punto débil de este tipo de firewall es que su seguridad puede ser vulnerada a través de código malicioso.

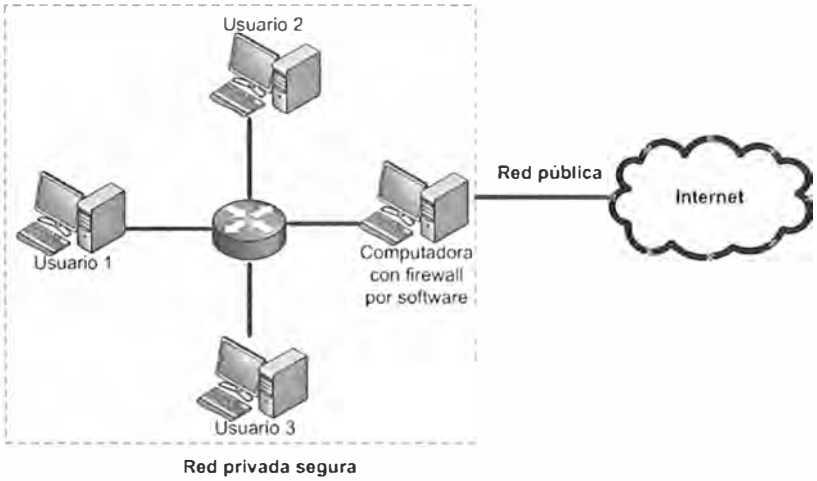


Fig. 3.25: Firewall por software

b. Firewall por hardware

Los firewalls basados en hardware pueden proteger a todos los equipos de la red (ver Fig. 3.26). Un firewall basado en hardware es más fácil de mantener y administrar que los firewalls de software individuales.

La solución ideal es un firewall de hardware integrado en una solución de seguridad completa. Para tener una seguridad integral además de firewall, la solución debe incluir una red privada virtual (VPN), antivirus, antispam, antispyware, filtrado de contenidos, y otras tecnologías de seguridad.

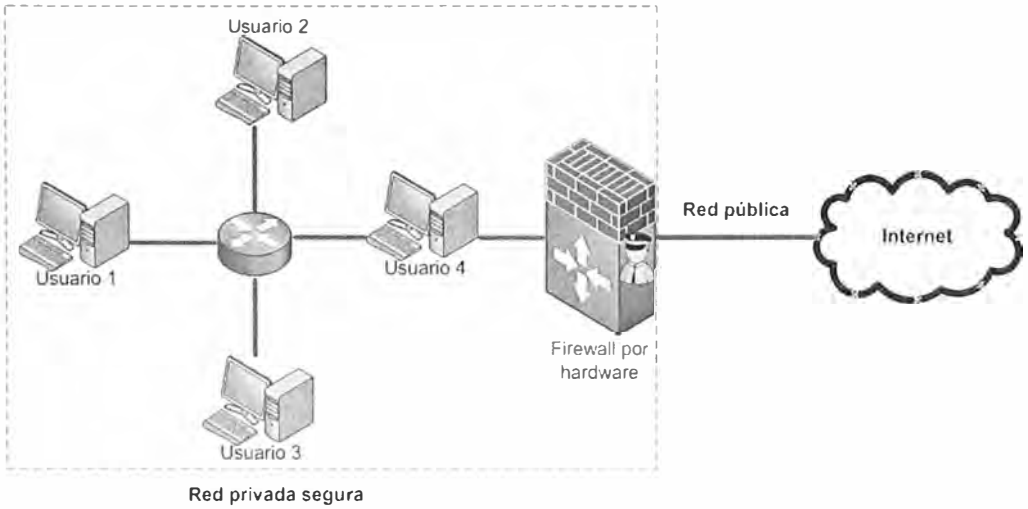


Fig. 3.26: Firewall por hardware

3.11.3 Tipos de configuración

Los tipos de configuración, son [12]:

a. Screened Host:

Es un equipo que protege una máquina de ataques externos, a través de un filtrado de paquetes.

Este filtrado en este configuración es básico, en esencia no acepta paquetes del exterior que no sean respuesta de una petición de una máquina interna.

b. Screened LAN:

Es similar al anterior, excepto que no protegemos una sola máquina, sino dos o más equipos (una red), este modelo no ofrece seguridad si el ataque es generado desde el interior a un equipo de la misma red.

c. Bastion Host

Esta configuración tiene características del screened host, con la diferencia que se permiten accesos desde afuera a ciertos servicios (SMTP, HTTP, DNS, etc.) en la red interna.

3.11.4 Limitaciones de los firewall

Los Firewalls no son sistemas inteligentes, ellos actúan de acuerdo a políticas y reglas pre-establecidas por el administrador de red, por consiguiente si un paquete de información no se encuentra dentro de estas reglas y políticas como una amenaza de peligro simplemente lo deja pasar. Más peligroso aún es que un intruso deje una puerta trasera, abriendo un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación es que el Firewall "No es contra humanos", es decir que si un intruso logra entrar a la organización y descubrir passwords o los huecos del Firewall y difunde esta información, el Firewall no se dará cuenta.

El Firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus, por lo que es altamente recomendable combinar el uso de firewall con antivirus apropiados.

3.11.5 Modelos OSI Y TCP / IP

Para entender cómo trabajan los firewalls se debe entender los distintos niveles de una red bajo el modelo OSI[13]. La arquitectura de red está basada en un modelo de siete niveles (ver Fig. 3.27). Cada nivel tiene su propio conjunto de responsabilidades, y se ocupa de ellos de una manera bien definida. Esto permite a las redes de mezclar y combinar protocolos de red y soportes físicos. En una red dada, un único protocolo puede viajar a más de un soporte físico (nivel uno), ya que el nivel físico se ha disociado de los niveles de protocolo (nivele tres a siete).

Los firewalls operan en diferentes niveles por que utilizan diferentes reglas para restringir el tráfico, en el protocolo de internet. De acuerdo al nivel se puede realizar el

enrutamiento de paquetes a su destino, en otro nivel un firewall puede determinar si un paquete es de una fuente confiable, pero no puede ocuparse de lo que contiene o lo que otros paquetes que está asociado. Los firewalls que operan en el nivel de transporte pueden conocer un poco más acerca de un paquete, y son capaces de conceder o denegar el acceso en función de criterios más sofisticados. A nivel de aplicación, los firewall saben mucho acerca de lo que está pasando y puede ser muy selectivos en la concesión de acceso.

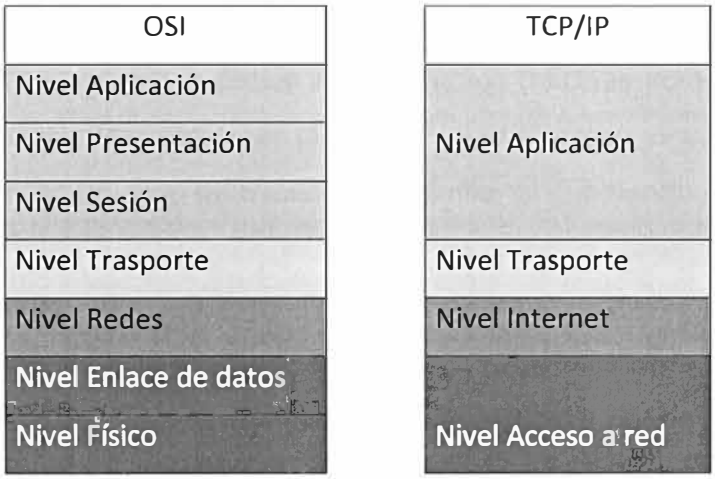


Fig. 3.27: Modelo OSI y TCP/IP

3.12Red privada virtual-VPN

Una VPN no es más que una estructura de red corporativa implantada sobre una red de recursos de carácter público, pero que utiliza el mismo sistema de gestión y las mismas políticas de acceso que se usan en las redes privadas, al fin y al cabo no es más que la creación en una red pública de un entorno de carácter confidencial y privado que permitirá trabajar al usuario como si estuviera en su misma red local (ver Fig. 3.28).

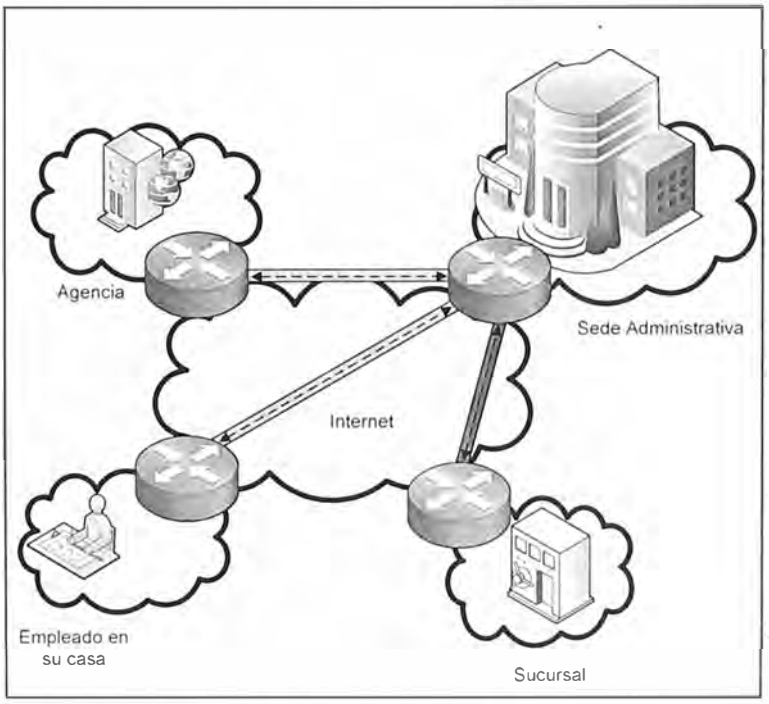


Fig. 3.28: Funcionamiento de una VPN

Desde el punto de vista del usuario que se conecta a ella, el funcionamiento de una VPN es similar al de cualquier red normal, aunque realmente para que el comportamiento se perciba como el mismo hay un gran número de elementos y factores que hacen esto posible.

3.12.1 Tipos de VPN

Los tipos de VPN son:

a. VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa.

b. VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales.

c. VPN over LAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

La comunicación entre los dos extremos de la red privada a través de la red pública se hace estableciendo túneles virtuales entre esos dos puntos y usando sistemas de encriptación y autentificación que aseguren la confidencialidad e integridad de los datos transmitidos a través de esa red pública. Debido al uso de estas redes públicas, generalmente Internet, es necesario prestar especial atención a las cuestiones de seguridad para evitar accesos no deseados.

En el traslado a través de Internet, los paquetes viajan encriptados, por este motivo, las técnicas de autenticación son esenciales para el correcto funcionamiento de las

VPNs, ya que se aseguran a emisor y receptor que están intercambiando información con el usuario o dispositivo correcto.

3.13 Zona desmilitarizada-DMZ

Una zona desmilitarizada (del inglés Demilitarized Zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet (ver Fig. 3.29).

El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, es decir: los equipos locales (hosts) en la DMZ no pueden conectar con la red interna.

Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de e-mail, Web y DNS.

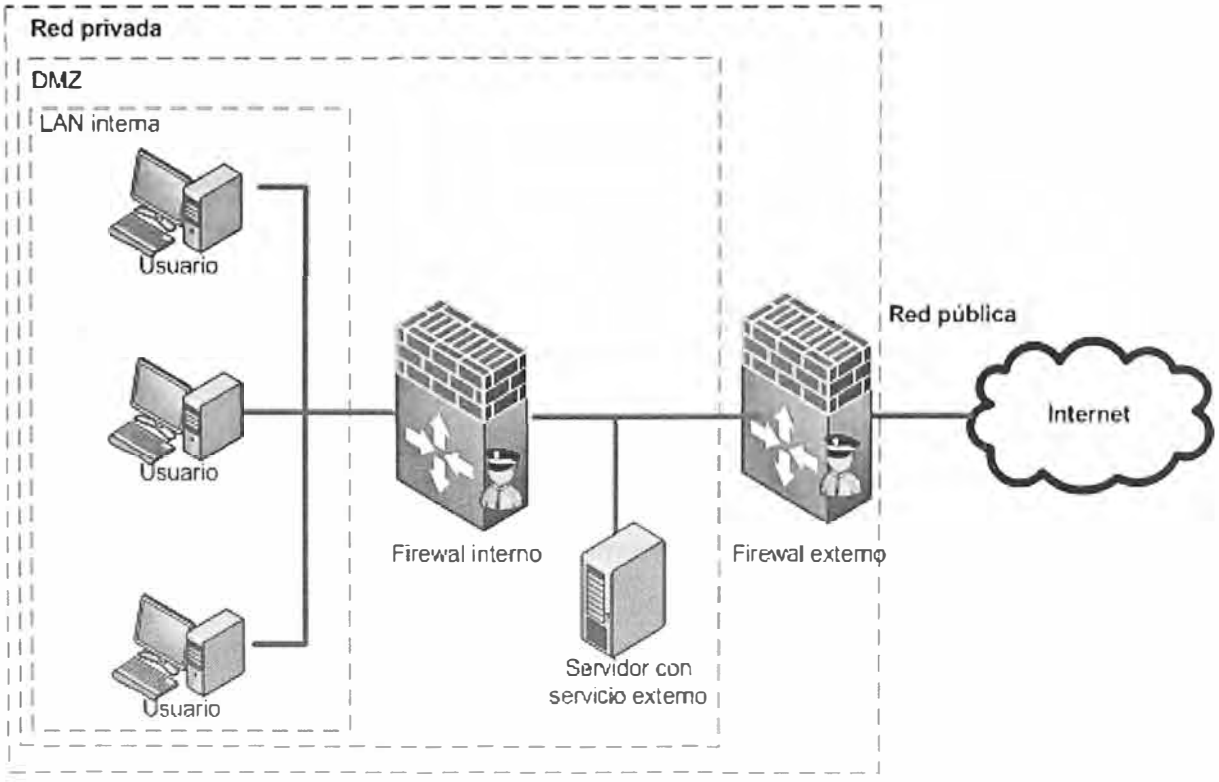


Fig 3.29: Funcionamiento de una DMZ

Las conexiones que se realizan desde la red externa hacia la DMZ se controlan generalmente utilizando Port Address Translation (PAT).

Habitualmente una configuración DMZ usa dos firewall, donde la DMZ se sitúa en medio y se conecta a ambos firewall, uno conectado a la red interna y el otro a la red

externa. Esta configuración ayuda a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna.

3.13.1 Caracteristicas de la DMZ

Las características de la DMZ son:

- Filtrado de paquetes a cualquier zona
- NAT, Mapeo Bidireccional
- Colas de tráfico y Prioridad
- Salidas redundantes / balanceo de carga
- Balanceo de carga a servicios
- Filtrado de contenido (web-cache)
- Monitoreo de tráfico en interfaces vía netflow

3.14Alta disponibilidad

Los sistemas de alta disponibilidad (high availability ó HA), están basadas en la replicación de elementos, naturalmente, si hablamos de replicar servidores, hablaremos de un clúster de alta disponibilidad.

En los sistemas de alta disponibilidad existen los tiempos de fuera de servicio; son mínimos pero existen, van desde 1 minuto o menos hasta 5 o 10 minutos, según sea el caso.

3.14.1 Tipos de alta disponibilidad

Son dos tipos [14]:

- Alta disponibilidad de infraestructura y
- Alta disponibilidad de aplicación.

A continuación se detallan cada una de ellas:

a. Alta disponibilidad de infraestructura:

Si se produce un fallo de hardware en alguna de los dispositivos del cluster, el software de alta disponibilidad es capaz de arrancar automáticamente los servicios en cualquiera de los otros dispositivos del cluster (failover) ubicados en otro lugar fuera del ambiente donde se produjo el fallo (normalmente a kilómetros de distancia). Y cuando la máquina que ha fallado se recupera, los servicios son nuevamente migrados a la máquina original (failback). Esta capacidad de recuperación automática de servicios nos garantiza la alta disponibilidad de los servicios ofrecidos por el cluster, minimizando así la percepción del fallo por parte de los usuarios.

b. Alta disponibilidad de aplicación:

Si se produce un fallo del hardware o de las aplicaciones de alguna de los dispositivos del cluster, el software de alta disponibilidad es capaz de arrancar automáticamente los servicios que han fallado en cualquiera de las otras máquinas del cluster. Y cuando la máquina que ha fallado se recupera, los servicios son nuevamente

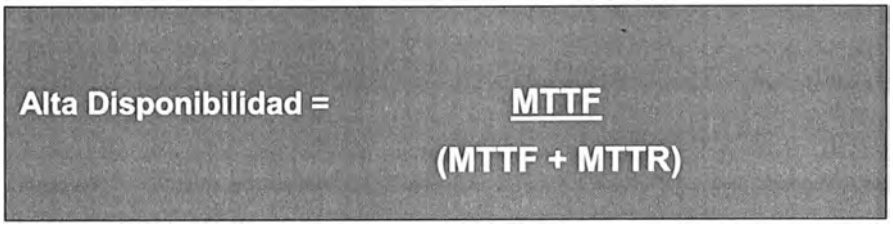
migrados a la máquina original. Esta capacidad de recuperación automática de servicios nos garantiza la integridad de la información, ya que no hay pérdida de datos, y además evita molestias a los usuarios, que no tienen por qué notar que se ha producido un problema.

3.14.2 Métricas de medición de alta disponibilidad

En un sistema real, si falla uno de los componentes, es reparado o sustituido por un nuevo componente. Si este nuevo componente falla, es sustituido por otro, y así sucesivamente. El componente fijo se considera en el mismo estado que un nuevo componente. Durante su vida útil, uno de los componentes pueden ser considerado en uno de estos estados: Funcionando o en Reparación. El estado funcionando indica que el componente está operacional y el estado en reparación significa que ha fallado y todavía no ha sido sustituido por un nuevo componente.

En caso de defectos, el sistema va de funcionando en modo reparación, y cuando se hace la sustitución volverá al estado funcionando. Por lo tanto, podemos decir que el sistema tiene durante su vida, una media de tiempo para presentar fallas MTTF(Tiempo medio entre fallas o mean time to failure en inglés) y un tiempo medio de reparación MTTR (Tiempo medio de recuperación o mean time to recover en inglés). Su tiempo de la vida es una sucesión de MTTFs y MTTRs, a medida que este va fallando y siendo reparado. El tiempo de vida útil del sistema es la suma de MTTFs en ciclos MTTF + MTTR ya vividos.

En forma simplificada, se dice que la disponibilidad de un sistema es la relación entre la duración de la vida útil de este sistema y de su tiempo total de vida. Esto puede ser representado por la fórmula siguiente que define la Alta Disponibilidad:



3.15 Niveles TIER

El estándar ANSI/TIA942[15] de Abril de 2005 (Telecommunications Infrastructure Standard for Data Centers) presenta una clasificación de cuatro niveles (Tiers) de la infraestructura de los Centros de Computo según el nivel de disponibilidad (ver TABLA Nº 3.8), siendo el TIER 1 el más sencillo y el TIER 4 el que tiene mayores redundancias. También hace una división de 4 subsistemas a saber: Arquitectónico, Eléctrico, Telecomunicaciones y Mecánico. Cada subsistema tiene los mismos cuatro niveles. El nivel total del centro de cómputo se da con el nivel del subsistema más bajo.

A continuación se presentan las características generales de cada uno de los niveles (Tiers) .

3.15.1 Nivel (TIER) 1. Básico

Sus características principales son:

- Rutas únicas de conexión a redes externas.
- Sin componentes redundantes.
- Es susceptible de interrupciones por actividades planeadas y no planeadas. Los UPS, aires y generadores son módulos simples y tienen múltiples puntos sencillos de falla. Las cargas criticas pueden ser expuestas a apagones durante mantenimientos preventivos o correctivos. Errores de operación o fallas espontaneas de los componentes de infraestructura causaran interrupciones en el centro de cómputo.

3.15.2 Nivel (TIER) 2. Redundante

Sus características principales son:

- Rutas únicas de conexión a redes externas.
- Componentes redundantes.
- Son significativamente menos susceptibles de interrupciones que el Tier 1 por actividades planeadas y no planeadas. El diseño de UPS y generadores necesita redundancia N+1, pero tiene un solo camino de distribución. El mantenimiento de las rutas criticas de potencia y otras partes de la infraestructura, requerirán el proceso de "shutdown".

3.15.3 Nivel (TIER) 3. Concurrentemente mantenible

Sus características principales son:

- Sistema multimódulo.
- Rutas duales o múltiples de conexión a redes externas.
- Doble ruta de alimentación de potencia.
- Perdida de redundancia durante falla o mantenimiento.
- Permite realizar actividades de mantenimiento planeadas sin tener que suspender servicios de hardware. Esto incluye labores de mantenimiento preventivo, correctivo, adición o remoción de equipos. Tiene suficiente disponibilidad en uno de los caminos cuando se estén haciendo trabajos al otro. No queda con redundancia cuando se hacen esos trabajos. Normalmente se diseñó con opciones de convertirse en TIER 4 cuando las operaciones del negocio así lo exijan.

3.15.4 Nivel (TIER) 4. Tolerante de fallas

Sus características principales son:

- Múltiples rutas de conexión a redes externas.
- Componentes redundantes.
- Fuente dual de potencia critica garantizada.
- No hay pérdida de redundancia durante una falla sencilla o mantenimiento.

TABLA Nº 3.8: Niveles TIER

Tier	Disponibilidad	Tiempo de parada anual
Tier 1	99.671%	28.82 horas
Tier 2	99.741%	22.68 horas
Tier 3	99.982%	1.57 hora
Tier 4	99.995%	52.56 minutos

3.16Protocolo seguro de transferencia de hipertexto-HTTPS

El protocolo HTTPS utiliza certificados (certificados para dispositivos) SSL (Secure Socket Layer) [16] y un cifrado basado en SSL/TLS para crear un canal cifrado cuyo nivel depende del servidor remoto y del navegador(ver Fig 3.30, 3.31 y 3.32) utilizado por el cliente, https se utiliza para tráfico de información sensible ya que el protocolo HTTP no maneja cifrado de datos. Este proceso permite al usuario de una página que utiliza este servicio confiar en los datos proporcionados dentro de la misma, los datos que ingresen a la misma, serán de carácter privado. Los protocolos SSL brindan barreras contra la mira de los extraños, dando total seguridad en las páginas de Internet para toda aquella información que se comparte entre servidores y usuarios, sea privada, por lo que son esenciales para mantener cualquier tipo de dato protegido de manos ajenas.

El protocolo funciona como codificador de datos mediante el proceso de cifrado asimétrico, dejando que sea descifrado solamente por aquellos autorizados. El Protocolo Secure Socket Layer fue desarrollado por Netscape Communications Corporation, la versión actual es SSL v3.0, y fue desarrollado con el objetivo inicial de proteger transacciones comerciales, llevando ahora la seguridad de millones de usuarios que navegan en Internet y comparten información con múltiples fines

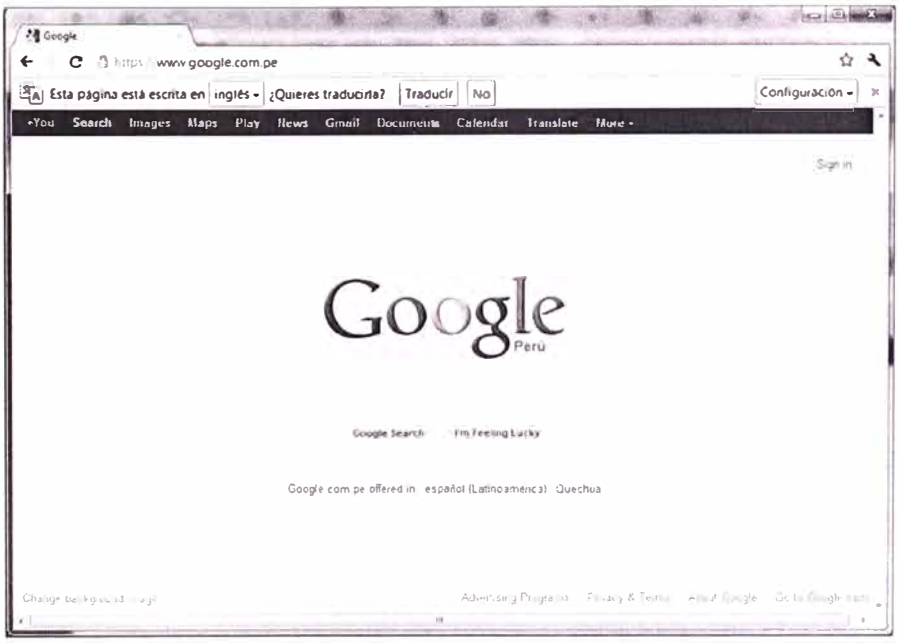


Fig. 3.30: Pagina web con conexión https

Fig. 3.31: Información de la conexión https

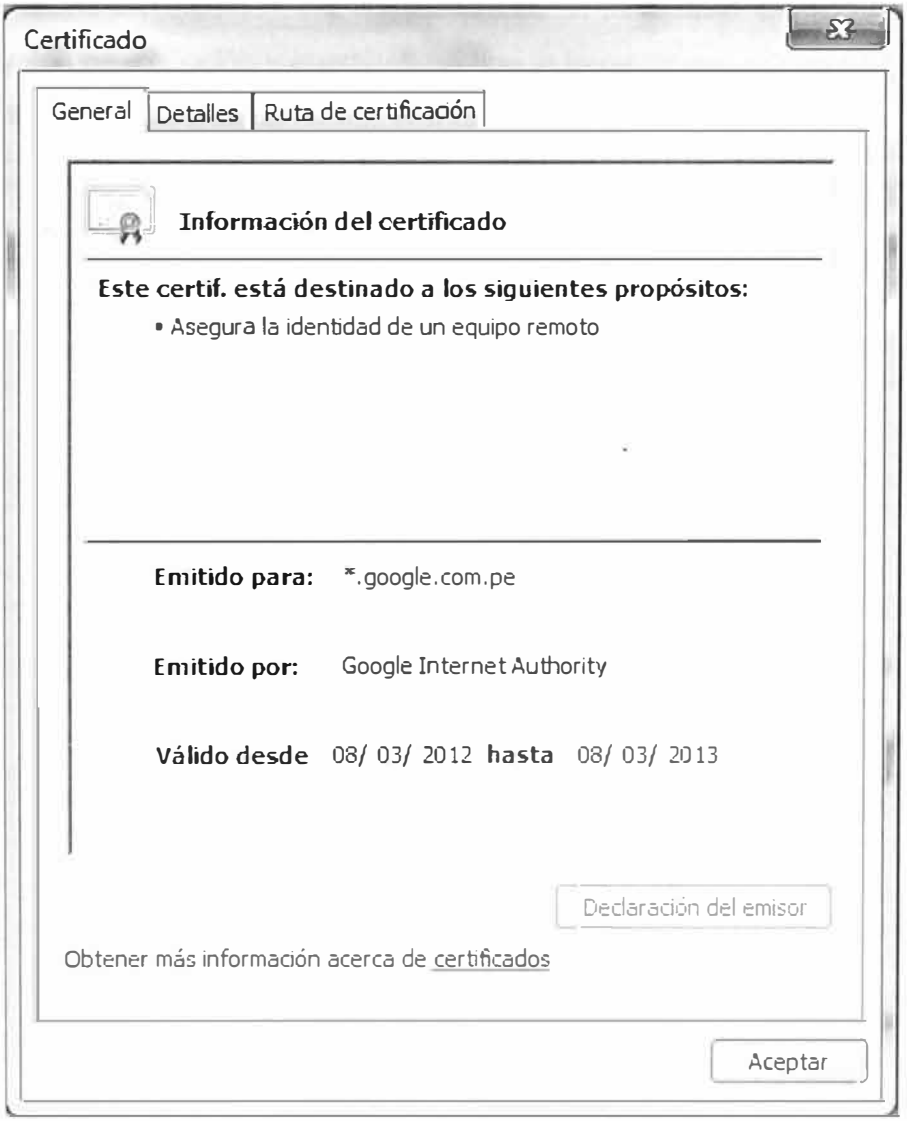


Fig.3.32: Certificado de conexion https

CAPITULO IV
INGENIERÍA DEL PROYECTO

En este capítulo se analizará el problema, se tomaran los datos del mismo, se utilizara una metodología y se diseñará la solución.

4.1 Situación actual

La entidad pública objeto de estudio, cuenta con una Sede Operativa en la ciudad de Lima, además cuenta con una Sede Administrativa también en la ciudad de Lima, ambas sedes están separadas por 5 K.m. de distancia.

Conforme su Ley Orgánica, es autónoma con atribuciones exclusivas y excluyentes en materia registral, técnica, administrativa, económica y financiera

La entidad pública en mención ha adoptado una organización gerencial a fin de potenciar sus niveles de ejecución y coadyuvar a que la toma de decisiones se realice en forma rápida y eficaz, asegurando el cumplimiento de los objetivos institucionales.

La organización gerencial permite contar con una estructura orgánica moderna, ágil, flexible, plana y con cadena de mando corta (ver Fig 4.1):

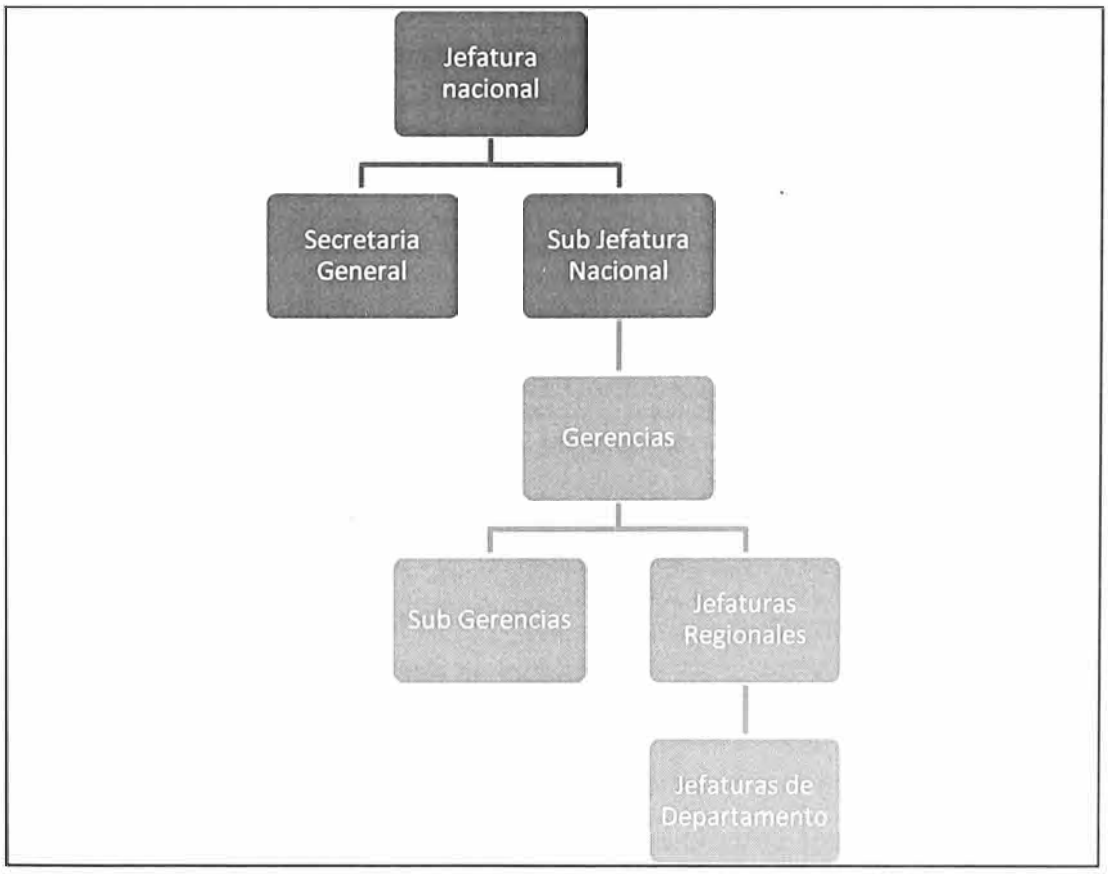


Fig. 4.1: Organigrama gerencial de la entidad

Ha sido designada con Entidad de Certificación, por lo que puede emitir certificados digitales como el valor legal y jurídico en todo el territorio nacional.

Como parte de su cartera de servicios, está dentro de sus planes brindar el servicio de sello de tiempo, para lo cual debe realizar el proceso de acreditación ante INDECOPI como una Entidad prestadora del Servicio de Valor Añadido (SVA) [16].

Esta entidad, en su propósito de brindar el servicio de certificación digital como Entidad de Certificación, y para disminuir la brecha digital de los ciudadanos, se ha visto en la necesidad de implementar un centro de datos principal para la emisión de certificados digitales, pero esto es insuficiente si es que no se brindan servicios en línea que el ciudadano pueda utilizar (tales como pago de impuestos, reserva de citas, etc.) en los cuales se usen los certificados digitales; pero para poner estos servicios a disposición del ciudadano es necesario que se cumplan que los criterios de: confidencialidad, integridad, disponibilidad, no repudio y hora exacta (esto con el fin de dar la total seguridad tanto legal como tecnológica que nadie va a poder alterar la información de la misma o suplantar la identidad del ciudadano), si se logra esto, de manera directa se tendrá un gobierno más ágil, orientado al ciudadano y también se percibirá como efecto inmediato una mejora en la calidad de vida de los ciudadanos (ya que hay un ahorro de tiempo y dinero, en la actualidad hay colas innecesarias, gasto en trasporte de un sitio a otro, etc.).

En el Estado Peruano todavía no existe entidad alguna que brinde el servicio de sello de tiempo, por lo que este trabajo, que consiste en el diseño de un red de comunicaciones para el servicio de sello de tiempo, proceso de funcionamiento del servicio de sello de tiempo y procedimiento de acreditación, servirá como referencia para la implementación de este servicio en cualquier entidad de características similares.

4.1.1 Centro de datos

El centro de datos de la entidad púbica que es objeto del presente análisis, es el corazón de las operaciones de la Entidad de Certificación, por lo que cuenta con diversas medidas de seguridad tanto física y lógica, tales como:

- Controles de acceso
- Sistemas de respaldo
- Procedimientos de copias de seguridad,
- Sistemas de control y prevención de incendios
- Sistema de videovigilancia, etc.

Además de una infraestructura que permite brindar sus servicios de acuerdo los niveles de disponibilidad, en la Fig. 4.2 se muestra el organigrama funcional del centro de datos.

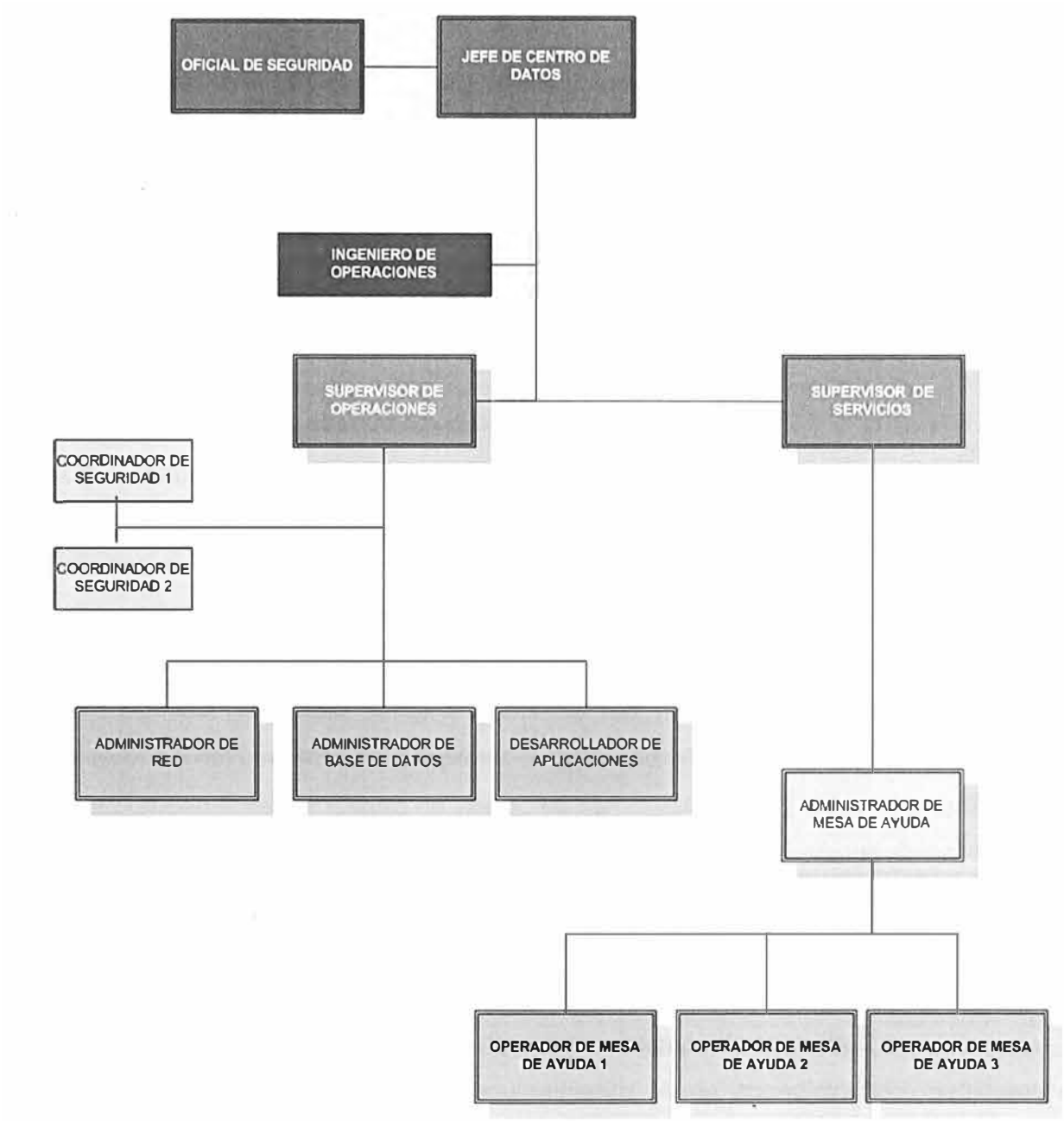


Fig 4.2: Organigrama funcional del centro de datos

Actualmente se ha implementado lo siguiente en el Centro de Datos:

- Acondicionamiento de la infraestructura de paredes.
- Acondicionamiento de la infraestructura de techos.
- Acondicionamiento de la infraestructura de piso técnico.
- Acondicionamiento de la infraestructura de falso cielo.
- Acondicionamiento de la infraestructura de luminosidad.
- Sistema eléctrico independiente del suministro del edificio del centro de datos, respecto a la red de distribución del edificio, luminarias, tomacorrientes para uso común, sensores, alarmas, sistema contra-incendios y otros dentro del Centro de Datos.
- Tomas de datos y tomas eléctricas dentro de Centro de Datos alimentados del sistema de UPS.

- Sardineles de delimitación.
- Soporte de todo el equipamiento(A/A, Servidores, UPS, trafos, etc.) a las paredes, pisos o techos de cemento de tal manera que se asegure su estabilidad en caso de sismo.
- Rampa con piso antiestático.
- Puerta de acceso al área principal.
- Falso cielo.
- Piso Técnico.
- Sala de máquinas y sala de operadores.
- Un sistema de aire acondicionado de precisión, funcionado con tres módulos en operación redundante con uno de ellos en stan-by de manera rotativa. Las mediciones de temperatura se realizan conforme a las normas ASHRAE. El ciclo del aire es tipo Down Flow (descarga de aire por debajo de piso técnico).
- Los equipos de Aire Acondicionado de Precisión propuestos están conectados directamente vía cable serial o cable de red hacia la central de alarmas y hacia el terminal del operador para reportar su actividad y/o alarmas.
- Los componentes del Centro de Datos, se han clasificado en: Infraestructura, Sistema de seguridad física, Sistema eléctrico y de protección, Cableado de datos, Hardware y software, Redes y comunicaciones y Seguridad TI, esta clasificación y los sub componentes de la misma se detallan en la Tabla Nº 4.1.

4.1.2 Sistema de seguridad

El Centro de datos cuenta con los siguientes sistemas de seguridad:

- Prevención antisísmica, todo el equipamiento (Airea acondicionado, gabinetes de servidores, UPS, trafos, etc.) están sujetados a las paredes, pisos o techos de cemento de tal manera que se asegure su estabilidad en caso de sismo.
- Sistema de control de acceso mediante tarjeta de proximidad
- Sistema de control de acceso biometrico
- Sistema de prevención y extinción de fuegos que se implementó siguiendo los lineamientos de la Normas NFPA 72 (National Fire Alarm Code) y NFPA 70 (NEC).
- Luces de Emergencia
- Un sistema de extinción de fuego, por Agente Limpio heptafluoruropropano (FM-200) para las instalaciones críticas. Un sistema de video-vigilancia permite registrar las imágenes en un sistema digital con cámaras IP que captan las imágenes durante las 24 horas del día, los 365 días del año. En la Tabla Nº 4.1, se muestra un resumen de los componentes del Centro de Datos.

Tabla Nº 4.1: Componentes del Centro de Datos

Categoría	Sub Categoría
Infraestructura	Albañilería
	Tabiquería
	Puertas
	Falso Cielo
	Piso Técnico
	Mamparas
	Sistema de Refrigeración
Sistema de seguridad física	Bases antisísmicas
	Sistema de control de acceso
	Sensores, paneles y alarmas
	Luces de emergencia
	Sistema de Extinción de Fuego
	Controles de apagado
	Sistema de Video-vigilancia
Sistema eléctrico y de protección	Tableros Eléctricos
	Aterramiento del Centro de Datos
	Aterramiento de gabinetes del Centro de Datos.
	Transformador de aislamiento
	Sistema de UPS´s
Cableado de datos	Cableado estructurado
	Tomas de datos
	Fibra óptica
Hardware y software	Software PKI
	Hardware PKI
	Hardware de servidores
	Software de servidores
	Bases de datos
	Estaciones de usuario
	Plataforma centralizada de incidentes, reportes y alarmas
	Sistema de almacenamiento externo (SAN)
	Almacenamiento en cinta magnética
Redes y comunicaciones	Routers
	Switch
Seguridad TI	Firewalls

4.1.3 Sistema eléctrico y de protección

El Centro de datos cuenta con un sistema eléctrico y de protección que tiene las siguientes características:

- Tableros eléctricos secundarios.
- Llaves de distribución.

- Tableros eléctricos principal.
- Total independencia del sistema eléctrico respecto a otros circuitos eléctricos del edificio.
- Montantes eléctricas independientes para las cargas estabilizadas del Centro de Datos, el sistema de aire acondicionado de precisión y para los circuitos de iluminación y tomacorrientes de uso común dentro del ambiente del Centro de Datos.
- Equipos de protección eléctrica TVSS
- Transformador de aislamiento de 100 KVA.
- Sistema de UPS principal.
- Sistema de UPS de contingencia.
- Baterías de respaldo.
- Gabinetes aprobados según GR-63-CORE de Telcordia respecto de la protección física en caso de sismo.
- Tomas de datos categoría 6 tipo UTP del tipo LSZH (LowSmoke Zero Halogen), patch panel y faceplates con jacks categoría 6.

4.1.4 Sistemas de comunicaciones

El Centro de datos cuenta con un sistema de comunicaciones que tiene las siguientes características:

- Comunicaciones telefónicas.
- Telefonía fija: Se cuenta con un proveedor del servicio.
- Telefonía móvil. Se cuenta con un proveedor del servicio
- Comunicaciones vía redes telemáticas.
- Se cuenta con fibra óptica entre las dos sedes (sede administrativa y sede operativa).
- Cuenta con un proveedor del servicio de internet.

4.1.5 Disponibilidad del servicio

Se requiere brindar el servicio con una disponibilidad compatible con Tier 3 (Nivel de disponibilidad de 99.982% anual), con un máximo de 1.57 horas de parada al año de las operaciones del centro de datos y se ofrecerá bajo un horario 365x24.

4.1.6 Determinación de la demanda

Al ser un tema muy especializado y no existir estadísticas de años anteriores (ya que no existen entidades acreditadas ante INDECOPI que brinden el servicio de sello de tiempo) se ha realizado una proyección considerando un escenario muy limitado en el cual por cada certificado emitido (del cual si existen proyecciones) solo se realiza un servicio de sello de tiempo en el año, tal como podemos observar en la Tabla Nº 4.2:

Tabla Nº 4.2: Número de transacciones del servicio de sello de tiempo

Año	Numero de certificados [18]			Transacciones proyectadas	Tasa de crecimiento
	Persona natural	Persona jurídica	Total	Proyección	
2012	500000	2000	502000	502000	--
2013	1500000	25000	1525000	1525000	303.78%
2014	2300000	75000	2375000	2375000	155.74%
2015	3000000	100000	3100000	3100000	130.53%

4.2 Estructura de red actual

La estructura de la red actual de la entidad pública objeto de estudio se puede observar en la Fig. 4.3:

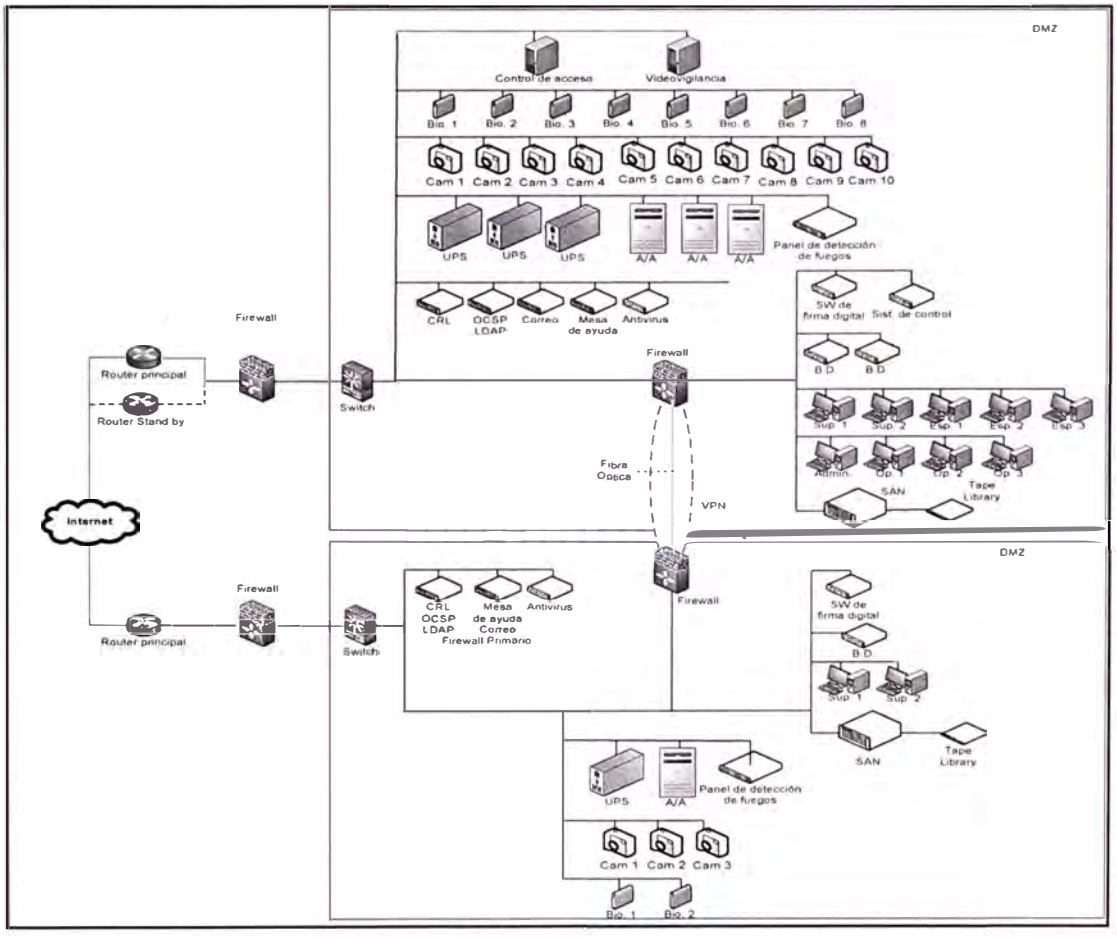


Fig. 4.3 Estructura actual de la red del centro de datos

4.3 Análisis y presentación del diseño

Antes de realizar el diseño, se va realizar primero un cronograma general de trabajo, el cual nos permitirá saber el estado actual del centro de datos.

4.3.1 Cronograma general de trabajo

El cronograma de trabajo es el que se detalla en la siguiente tabla:

TABLA Nº 4.2: Cronograma General de Trabajo

DISEÑO DE DIAGRAMA DE RED CON CRITERIOS DE ALTA DISPONIBILIDAD, REDUNDANCIA Y BALANCEO DE CARGA												
N°	Nombre de la tarea	Duración de la tarea (en días)										
		1d	2d	9d	9d	6d	6d	3d	144d	7d	7d	30d
1	FASE 1: ANÁLISIS DE BRECHA											
2	Identificación de dispositivos del diagrama de red actual											
3	Análisis de brecha											
4	**Entregable: Análisis de Brecha**											
5	FASE 2: ESPECIFICACIONES DE DISPOSITIVOS											
6	Determinación de características obligatorias de los dispositivos											
7	**Entregable: Documento de características obligatorias de dispositivos Firewall, balanceadores de carga y servidores NTP**											
8	Análisis de características de dispositivos disponibles en el mercado											
9	Identificación de características de mejoras adicionales de dispositivos											
10	Integración de características de los dispositivos											
11	**Entregable: Documento de Especificaciones de dispositivos**											
12	FASE 3: PROCESO DEL SERVICIO DE SELLO DE TIEMPO											
13	Desarrollo del proceso de sello de tiempo											
14	**Entregable: Proceso de Sello de Tiempo**											
15	Elaboración de diagrama de red con criterios de											

	Alta Disponibilidad, Balanceo de carga, Redundancia e Inclusión del servicio de Sello de Tiempo											
16	**Entregable: Diagrama de red con criterios de Alta Disponibilidad, Balanceo de carga, Redundancia e Inclusión del servicio de Sello de Tiempo**											
17	FASE 4: INTEGRACIÓN DE DISPOSITIVOS											
18	Integración de dispositivos al Centro de Datos, incluye: Proceso de licitación pública instalación y configuración.											
19	Integración del servicio de Sello de Tiempo											
20	**Entregable: Informe de integración y configuración de dispositivos y del servicio de sello de tiempo**											
21	Elaboración de la Estructura de plan de pruebas											
22	**Entregable: Plan de Pruebas**											
23	Ejecución de Plan de Pruebas											
24	**Entregable: Informe de pruebas y estado actual de los dispositivos y servicio de sello de tiempo**											

PROCESO DE ACREDITACIÓN COMO SVA DEL SERVICIO DE SELLO DE TIEMPO

N°	Nombre de la tarea	Duración de la tarea (en días)									
		8d	1d	1d	1d	5d	11d	20d	5d	10d	Xd
25	FASE 5: PLANIFICACIÓN DEL PROCESO DE ACREDITACIÓN										
26	Análisis de requerimientos de la Guía de Acreditación SVA										

27	Identificación de requerimientos										
28	Análisis de riesgos										
29	Elaboración del Plan de Acreditación										
30	**Entregable: Plan de Acreditación**										
31	FASE 6: EJECUCIÓN DEL PLAN DE ACREDITACIÓN										
32	Asignación de responsables del Plan de Acreditación										
33	Recopilación de registros del servicio de sello de tiempo										
34	Elaboración de la documentación										
35	Preparación de documentos del expediente										
36	Capacitación al personal										
37	Revisión de la documentación										
38	Auditorías internas										
39	Implementación de No conformidades, Oportunidades de Mejora identificadas en la Auditoría Interna										
40	**Entregable: Expediente de Acreditación**										
41	FASE 7: PROCESO DE ACREDITACIÓN COMO SVA										
42	Proceso de acreditación como SVA[1]										
43	**Entregable: Certificado de Acreditación como SVA expedido por INDECOPI**										

4.3.2 Fase 1: análisis de brecha

Se ha realizado un análisis de brecha, tomando los datos contenidos en los numerales

- 4.1.1 Centro de datos,
- 4.1.2 Sistema de seguridad,
- 4.1.3 Sistema eléctrico y de protección,
- 4.1.4 Sistemas de comunicaciones,

[1]La duración de este proceso depende de INDECOPI

- 4.1.5 Disponibilidad del servicio,
- 4.1.6 Determinación de la demanda,

Con la recolección de estos datos se puede realizar el análisis de brecha, el cual se presenta en la Tabla Nº 4.3:

TABLA Nº 4.3: Análisis de brecha

N°	Característica	Estado actual
1	Alta disponibilidad Infraestructura:	Cuenta con un centro de datos de contingencia Se cuenta con dispositivos: • Switch • SAN • Servidor de operaciones • Dispositivos biométricos • Cámaras de video-vigilancia • Servidor de mesa de ayuda
2	Alta disponibilidad Aplicación:	Cuenta aplicaciones propias del fabricante de los servidores, los cuales permiten el control y supervisión de los mismos.
3	Redundancia de equipos	Se cumple en criterio de redundancia para: • Switch • SAN • Servidores de operaciones • Dispositivos biométricos • Cámaras de video-vigilancia • Servidor de mesa de ayuda • Aire acondicionado • Energía eléctrica
4	Balanceo de carga	No cuenta con dispositivos balanceadores de carga
5	Sello de tiempo	No se cuenta con dispositivos NTP. No se cuenta con un proceso de sello de tiempo.
6	Disponibilidad del 99.982%	Se realizara las mediciones mensuales y anuales cuando el servicio entre a producción.
7	Rutas duales o múltiples de conexión a redes externas.	Se cuenta con: • Un proveedor de internet. • Un proveedor de telefonía fija. • Un proveedor de telefonía móvil
8	Doble ruta de alimentación de potencia.	Centro de datos principal. Cuenta un sistema de UPS, con una autonomía de 2 horas. Cuenta con un proveedor de energía eléctrica. Centro de datos de contingencia. Cuenta un sistema de UPS, con una autonomía de 40minutos.

9	Perdida de redundancia durante falla o mantenimiento	En la DMZ del centro de datos principal, está presente un firewall para la DMZ. Dos router, en el Centro de Datos principal En la DMZ del centro de datos de contingencia, se encuentran: Un firewall para la DMZ, en el Centro de Datos de contingencia Un router, en el Centro de Datos de contingencia
10	Permite realizar actividades de mantenimiento planeadas sin tener que suspender servicios de hardware. Esto incluye labores de mantenimiento preventivo, correctivo, adición o remoción de equipos.	El servicio continua disponible en el caso de: • Servidores de operaciones • Servidores de mesa de ayuda • Aire acondicionado • Sistema de video-vigilancia • Sistema de control de acceso • El servicio se suspende en el caso falla o mantenimiento de: • Sistema de seguridad de red (Firewall)
11	Tiene suficiente disponibilidad en uno de los caminos cuando se estén haciendo trabajos al otro.	Cuenta con un centro de datos de contingencia
12	No queda con redundancia cuando se hacen esos trabajos.	Cuenta con un centro de datos de contingencia

4.3.3 Determinación de las necesidades

Para cumplir los criterios de:

1. Alta disponibilidad.

   Se debe:

- Seleccionar dispositivos firewall internos de similares características y diseñarlos para que estén en configuración de alta disponibilidad.
- Seleccionar dispositivos firewall externos de similares características y diseñarlos para que estén en configuración de alta disponibilidad.
- Seleccionar dispositivos NTP y diseñarlos para que estén en configuración de alta disponibilidad.

2. Redundancia.

   Se debe:

- Seleccionar dispositivos firewall internos de similares características y diseñarlos para que estén en configuración de redundancia.
- Seleccionar dispositivos firewall externos de similares características y diseñarlos para que estén en configuración de redundancia.

- Seleccionar dispositivos balanceadores de carga y diseñarlos para que estén en configuración de redundancia.
- Seleccionar dispositivos NTP y diseñarlos para que estén en configuración de redundancia

3. Balanceo de carga.

   Se debe:

- Seleccionar dispositivos balanceadores de carga.

4. Sello de tiempo

   Se debe:

- Seleccionar dispositivos NTP de similares características.
- Elaborar el proceso de sello de tiempo.

4.3.4 Fase 2: especificaciones técnicas del equipamiento

Por tratarse de una institución pública, está prohibido de realizar compras directas de equipos, dispositivos o bienes orientados a una marca o proveedor[2], por lo que se plantea utilizar la siguiente metodología (ver Tabla Nº 4.4) para la determinación de las características de dispositivos:

Tabla Nº 4.4: Metodología para especificación de dispositivos

Pasos	Descripción
1	Determinación de las características requeridas de los dispositivos.
2	Identificación de dispositivos presentes en el mercado.
3	Selección de dispositivos que cumplen con las características
4	Identificación de características con mejoras adicionales de dispositivos seleccionados.
5	Integración de las características.

Además para una mejor identificación de las características se utiliza la siguiente secuencia de colores:

1. Características necesarias (color negro)
2. Características a integrar (color azul oscuro)
3. Características a descartar (color rojo oscuro)

a. Características de dispositivo firewall

Las características de los dispositivos firewall se describen a continuación, estas características son necesarias para el funcionamiento correcto del servicio de sello de tiempo y son:

---

[2] Ley N°. 340-06 sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones CAPÍTULO II Art. 3. Principio de igualdad y libre competencia

- Sistema grafico de control de ancho de banda
- Sistema gráfico de monitoreo de estados de los Firewalls.
- Firewall con soporte a Alta Disponibilidad.
- Inspección para el tráfico de aplicaciones Web y protección contra ataques a nivel de aplicación.
- Soporte de protocolos de entunelamiento: IPSEC
- Soporte de emisión de certificados digitales X.509 tanto para los módulos de cada firewall, como para los clientes de que acceden vía VPN.
- Sistema Operativo debe residir en un servidor de tipo appliance de la misma marca del software.
- Throughput mínimo de 1Gbps para el firewall de perímetro e interno
- Interfaces de red con velocidades de 10/100/1000
- Appliance con sistema operativo propietario configurado en alta disponibilidad y tolerancia a fallas.

b. Características de dispositivos presentes en el mercado

Se han analizado dispositivos firewall, por hardware y por software.

Según la página web All internet Security[19], en la categoría de firewall por software se encuentran en el puesto 1 y 2 respectivamente:

- Zone Alarm PRO Firewall de Check Point Software Technologies Ltd[20].
- Panda Global Protection 2012 de Panda Security 2012[21].

Para los firewall por hardware se han seleccionado los equipos:

- FORTINET 310B de FORTINET, Inc[22].
- JUNIPER IDP75 Juniper Networks, Inc[23].
- Check Point 2200 de Check Point Software Technologies Ltd[24].

En análisis se ha realiza en base a la información disponible (brochure, información del fabricante en internet, etc.) y se presenta en la Tabla Nº 4.5:

Tabla Nº 4.5: Características dispositivos firewall presentes en el mercado

Características	FORTINET 310B	JUNIPER IDP75	Check Point 2200	Zone Alarm PRO Firewall	Panda Global Protection 2012
					
Sistema grafico de control de ancho de banda	Si	Si	Si	Si	Si
Sistema gráfico de monitoreo de estados de los Firewalls.	Si	Si	Si	Si	Si

Firewall con soporte a Alta Disponibilidad.	Si	Si	Si	No	No
Inspección para el tráfico de aplicaciones Web y protección contra ataques a nivel de aplicación.	Si	Si	Si	Si	Si
Soporte de protocolos de entunelamiento: IPSEC	Si	Si	Si	No	No
Throughputpara el firewall de perimetro e interno	8 Gbps	10Gbps	3Gbps	No	No
Interfaces de red con velocidades de 10/100/1000	Si	Si	Si	No	No
Appliance con sistema operativo propietario configurado en alta disponibilidad y tolerancia a fallas.	Si	Si	Si	No	No
Licencia de actualización de signatures (actualización de parches y upgrades de versión del producto)	Si	Si	Si	Si	Si
Número de conexiones simultáneas.	500000	No indica	1.200000	No	No
Soporte de protocolo NTP	Si	No indica	Si	No	No
Soporte de emisión de certificados digitales X.509 tanto para los módulos de cada firewall, como para los clientes de que accedan vía VPN	Si	Si	Si	No	No
Sistema Operativo debe residir en un servidor de tipo appliance de la misma marca del software.	Si	Si	Si	No	No
Dispositivo IPS integrado	Si	No	Si	No	No
Acceso Mobil	No	No	Si	No	No
Funcionescomo DLP	No	No	Si	No	No
Antivirus & Anti-Malware	No	No	Si	No	No
Anti-Spam& Email Security	No	Si	Si	No	No
Detección de trafico MPLS	No	Si	No	No	No
Soporte para sistemas de autenticación: RADIUS, TACACS/TACACS	Si	No	No	No	No
Soporte de VoIP con los siguientes protocolos: H.323, MGCP, SCCP (Skinny) y SIP.	No	No	No	Si	Si
Sistema de administración centralizada	Si	Si	Si	No	No
Modulo de integración de los usuarios del servicio de acceso remoto (VPN) y el sistema de directorio de red Active Directory.	Si, con la utilidad AutoIKE	Si	No	No	No
Módulos de autenticación de los usuarios VPN con el sistema de Directorio Activo	Si	Si	No	No	No
La solución de clientes del servicio de VPN deberá ser compatible con las	No indica	Si	No indica	No indica	No indica
Fuente de poder: 220 VAC y 60 Hz.	Si	Si	Si	No	No
Fuente de poder redundante	No	Si	Si	No aplica	No aplica
Capacidad de integración con los IPS	SI, es un apliance	Si	Si	No indica	No indica
VLANS	No indica	No indica	1024	No	No
Storage	**250GB**	**No indica**	**250GB**	**No aplica**	**No aplica**

Certificaciones de seguridad:	ICSA Labs: Firewall, IPSec	No indica	UL, cUL, CB, CE, FCC, TUV, VCCI, C-Tick, RoHS		
Antivirus, IPS, Antispyware	Si	No	No	No	NO
Cumplimiento de estandares internacionales:UL/CUL, C Tick, VCCI	FCC Class A Part 15,	FCC class A	No indica	No	No
Puertos USB	No indica	No indica	2	No	No
Mean Time BetweenFailures	No indica	75000h	No indica	No	No aplica

c. Integración de características de dispositivos firewall

Finalmente se van a integrar las características del dispositivo firewall:

1. Sistema grafico de control de ancho de banda
2. Sistema gráfico de monitoreo de estados de los Firewalls.
3. Inspección para el tráfico de aplicaciones Web y protección contra ataques a nivel de aplicación.
4. Soporte de protocolos de entunelamiento: IPSEC
5. Firewall con soporte a Alta Disponibilidad.
6. Throughput mínimo de para el firewall de perímetro e interno de 3Gbps
7. Interfaces de red con velocidades de 10/100/1000
8. Appliance con sistema operativo propietario configurado en alta disponibilidad y tolerancia a fallas.
9. Licencia de actualización de signatures (actualización de parches y upgrades de versión del producto)
10. Número mínimo de 500000 de conexiones simultáneas.
11. Soporte de protocolo NTP
12. Soporte de emisión de certificados digitales X.509 tanto para los módulos de cada firewall, como para los clientes de que acceden vía VPN.
13. Dispositivo IPS integrado
14. Sistema Operativo debe residir en un servidor de tipo appliance de la misma marca del software.
15. Anti-Spam & Email Security
16. Sistema de administración centralizada .
17. Modulo de integración de los usuarios del servicio de acceso remoto (VPN) y el sistema de directorio de red Active Directory.
18. Módulos de autenticación de los usuarios VPN.
19. Fuente de poder: 220 VAC y 60 Hz.
20. Fuente de poder redundante
21. Capacidad de integración con los IPS

22. Storage mínimo de 250 GB
23. Certificaciones de seguridad: FCC, CE
24. Cumplimiento del estandar FCC Class A o similares

d. Características del equipo servidor horario NTP.

Para el caso del servidor NTP, al tratarse de un dispositivo muy especializado, existen pocas marcas presentes en el mercado, además no existe un software que pueda realizar las funciones de servidor NTP (por el uso del oscilador de Rubidio; no se debe confundir con la existencia de software cliente NTP), las características necesarias son las siguientes:

1. Conexión GPS
2. Tipo de enclosure: Rack
3. Nivel de Stratum 1
4. Cumplimiento de IP versionv4 y IPv6
5. Tipo de Oscilador: Rubidio
6. Tipo de antena: GPS
7. Cumplimiento de NTP v4.0
8. Certificaciones como mínimo: FCC y CE
9. Autenticación MD5 (RFC 1321)
10. Precisión mínimo de 2 milisegundos en LAN
11. Soporte mínimo para 1000 clientes NTP
12. Mínimo satélites por tiempo: 1 intermitente
13. Canales de recepción GPS

e. Características de servidores NTP

En el caso de los servidores NTP, analizaremos los existentes en el mercado:

- Symmetricom NTP 150 de Symmetricom, Inc [25].
- LANTIME M300/GPS de MeinbergFunkuhrenGmbH& Co. [26].
- NTS-6001 de GalleonSystem[27].
- Tempus LX GPS NTP de EndRun Technologies[28].

El análisis de los servidores NTP se muestra en la Tabla Nº 4.6:

Tabla Nº 4.6: Características de servidores NTP presentes en el mercado

Características	Symmetricom NTP 150[10]	LANTIME M300/GPS	NTS-60001	Tempus LX GPS Network Time Server
				
Conexión GPS	GPS	GPS	GPS	GPS

Tipo de enclosure: Rack	Rack	Rack	Rack	Rack
Nivel de Stratum 1	Stratum 1	Stratum 1	Stratum 1	Stratum 1
Cumplimiento de IPversionv4 y IPv6	IPversionv4 y IPv6	IPversionv4 y IPv6	IPversionv4 y IPv6	IPversionv4 y IPv6
Tipo de Oscillador	OCXO o Rubidium	OCXO o Rubidium	No indica	OCXO o Rubidium
Tipo de antena	GPS	GPS	GPS	GPS
NTP v4.0	v4.0 y 3.0	v4.0	v4.0 y 3.0adicionalmente soporte v2.0	v4.0 y 3.0
Certificaciones como mínimo: FCC y CE	FCC y CE	FCC y CE	FCC y CE	FCC y CE
MD5 Authentication (RFC 1321)	Si	Si	Si	Si
Precisión mínimo de 2 milisegundos en LAN	1-2 ms	1-2 ms	1-10 ms	Si, 30 ns
Soporte mínimo para 1000 clientes NTP	1600 clientes NTP	No indica	1000 clientes NTP segundo	200000 clientes NTP
Mínimo satélites	1 satélite	1 satélite	1 satélite	No indica
Canales de recepción GPS	12 canales de recepción	6 canales de recepción	12 canales de recepción	8 canales de recepción
Número de puertos de conexión	2 RJ45	2 RJ 45 de 10/100 Mbit	2 RJ45	1 RJ45
Extensión de de cable categoría 5	15 m	20m	10m	No indica
Serial: Bi-directional RS-232	RS-232	RS-232	No indica	RS-232

Cumplimiento de protocolos	SNTP, TIME (RFC 868), DAYTIME (RFC 867), Telnet (RFC 859), FTP (RFC 959), SNMP (RFC 1157), MIB II (DHCP (RFC 2132)	No, no soporta protocolos: DAYTIME MIBII Adicionalmente soporte SysLOG, FTP	SNTP, TIME (RFC 868), DAYTIME (RFC 867), Telnet (RFC 859), FTP (RFC 959), SNMP (RFC 1157), DHCP (RFC 2132)	SNTP, TIME (RFC 868), DAYTIME (RFC 867), Telnet (RFC 859), FTP (RFC 959),
Peticiones NTP por segundo	40 por segundo	No indica	No indica	20 por segundo
Precisión <1 microsegundo para UTC	<1us	<1us	<1us	< 100 ns
Network: 10/100Base-T Ethernet: RJ-45	Si	Si	Si	Si
Tipo de Display	LCD Display	LCD Display	LCD Display	LCD Display
Cliente	Windows XP y superiores	No, utiliza Linux	Windows XP y superiores	Si, además de Linux
Upgrade a osciladores de Rubidio	Si	Si	No indica	No indica
Alimentación	100-240 V, 60 Hz	100-240 V, 60 Hz	100-240 V, 60 Hz	Si,- 90-264 VAC, 47-63 Hz

f. Integración de características de los servidores NTP

Finalmente las características de los servidores NTP son:

1. Conexión GPS
2. Tipo de enclosure: Rack
3. Nivel de Stratum 1
4. Cumplimiento de IP versionv4 y IPv6
5. Tipo de Oscillador Rubidio
6. Tipo de antena: GPS
7. NTP v4.0 y adicional NTP v3.0
8. Certificaciones como mínimo: FCC y CE

9. Autenticación MD5 (RFC 1321)
10. Precisión mínimo de 1-2 milisegundos en LAN
11. Soporte mínimo para 1000 clientes NTP
12. Mínimo satélites por tiempo: 1 intermitente
13. Mínimo de 6 Canales de recepción GPS
14. Mínimo de 2 puertos RJ45
15. Mínimo de 10m de cable categoría 5
16. Cumplimiento de protocolos: SNTP, TIME (RFC 868), DAYTIME (RFC 867), Telnet (RFC 859), FTP (RFC 959), SNMP (RFC 1157), DHCP (RFC 2132)
17. Serial: Bi-directional RS-232
18. Precisión <1 microsegundo para UTC
19. Network: 10/100Base-T Ethernet: RJ-45
20. Tipo de Display: LCD
21. Cliente para Windows XP y superiores, opcionalmente para Linux
22. Alimentación 100-240 V, 60 Hz

g. Características de los dispositivos balanceadores de carga

Las características de los dispositivos balanceadores de carga se describen a continuación, estas características son necesarias para el funcionamiento correcto del servicio de sello de tiempo y son:

1. Throughput mínimo de 1.0 Gbps
2. Mínimo 400 SSL TPS
3. Compresión por hardware 1Gbps
4. Switching a nivel de capa
5. Mínimo 5M de sesiones simultaneas
6. Procesador: core 2
7. Memoria mínima de 4GB
8. Puertos: Gigabit/GBIC Ports
9. Certificación: EN 60950; UL 1950, FCC, Part 15B Class A, CE
10. Estandares: FCC Part 15B Class B

h. Características de dispositivos presentes en el mercado

Se ha realizado un análisis de las características de dispositivos balanceadores de carga, tomando en cuenta las marcas más conocidas en el mercado, tales como:

- Radware APP 2016 de Radware Ltd[29].
- BIG-IP 8950 de F5 Networks, Inc[30].
- Barracuda 640 de Barracuda Networks, Inc[31].
- Coyote Point E650GX de Coyote Point Systems [32].

El análisis se muestra en la Tabla Nº 4.7:

Tabla Nº 4.7: Dispositivos balanceadores de carga presentes en el mercado

Características	Radware APP 2016	BIG-IP 8950	Barracuda 640	Coyote Point E650GX
				
Throughput	1.2Gbps	20Gbps	950Mbps	1.3 Gbps
Minimo400 SSL TPS	500 SSL TPS	500 SSL TPS	200 SSL TPS	1400 SSL TPS
Compresión por hardware 1Gbps	Si, 500 Mbps escalable a 1 Gbps	No	No indica	1Gbps
Switching a nivel de capa	Capa 2	Capa 4 y7	Capa 4 y 7	Capa 4 y 7
Minimo 5M de sesiones simultaneas	8 millones	No indica	No, 250	Ilimitado
Procesador core 2	Core 2	Dual CPU, QuadCore (8 procesadores)	Core 2	Dual CPU, Quad Core (8 processors)
Memoria mínima de 4GB	4GB	16 GB	No indica	16 GB
Gigabit/GBIC Ports	2 Ge + 2 SFP	16 Ge + 2 SFP	1 Ge + 1 SFP	20 x GigE (1000 base-T) 2 x GigE SFP
Certificación:	EN 60950; UL 1950, CSA 22.2 No 950 EMI: EN 5022 Class A, EN 50024 FCC, Part 15B Class ACE,CUL,	CSA C22.2 No. 60950-1-03UL 60950-1:2001, 1st edition CSA C22.2 No. 60950-1-03IEC 60950-1: 2005, 2nd edition EN 60950-1: 2005, 2nd edition	IEC 60950-1UL 60950-1:2001	FCC, CFCC, UL, CAN/CSA, CE, VCCI, CB, IEC950, RoHS.

Estandares: FCC Part 15B Class B	EMI: EN 55022, FCC Part 15B Class B	EN 55022:2006 + C1:2006 EN 55024:1998 +A1: 2001 A2:2003,FCC Part 15B Class AVCCI Class A	FCC Part 15B Class A	FCC, CFCC, UL, CAN/CSA, CE, VCCI, CB, IEC950, RoHS.
Disco duro	No indica	No indica	No indica	2 discos de 320 GB
Protocolos de routeo	OSPF, RIP, RIP II	No indica	No indica	No indica
Compresión por software	No	No	No	Included: 50 Mbps Maximum: 8 Gbps
Fuente de poder	Simple	Simple	Simple	Doble fuente de 850W
Puerto USB	Si	Si	SI	Si
LCD Screen	Si	Si	SI	Si
Alimentación: 220v , 60 Hz	120/250 VAC	120/240 VAC	Si	Si, 120/240 VAC autodeteccion50/60Hz
Fuente de poder doble	Si	Si	Si	No indica
Topología de red	Full-NAT, Half-NAT, 802.1Q	Full-NAT, Half-NAT, 802.1Q	NO indica	Full-NAT, Half-NAT, 802.1Q (Tagged VLAN), Direct Server Return (DSR)
Aplicaciones soportadas	No indica	No indica	No indica	SSL VPN, Database
Metidos de persistencia	No indica	No indica	No indica	Cookies, client IP, client network, header match rules.
Algoritmo de compresión	No indica	No indica	No indica	GZIP.
Datos comprimidos	No indica	No indica	No indica	HTML, Office Document, Executables (.Exe).

Funciones criptográficas soportadas	HTTPS, Secure Sockets Layer (SSL), Transport Layer Security	(TLS), AES (128 and 256 bit), DES, 3DES, RC4, SHA-1, MD5, RSA		HTTPS, Secure Sockets Layer (SSL), Transport Layer Security (TLS), AES (128 and 256 bit), DES, 3DES, RC4, SHA-1, MD5, RSA.
Administración	HTTPS) Load Balancing Specific SNMP MIB Command Line	HTTPS) Load	HTTPS)	Secure Web based administration and management GUI (HTTP/HTTPS) Load Balancing Specific SNMP MIB Command Line Interfaces via Serial and SSH.

i. Integración de características de los dispositivos balanceadores de carga

Finalmente las características de los dispositivos balanceadores de carga son:

1. Throughput mínimo de de 1.0 Gbps
2. Mínimo 500 SSL TPS
3. Compresión por hardware
4. Switching a nivel de capa 2, 4 o 7
5. Mínimo 5M de sesiones simultaneas
6. Tipo de procesador : mínimo core 2
7. Memoria mínima de 4GB
8. Puertos: Gigabit/GBIC: mínimo 1 Ge + 1 SFP
9. Certificación: FCC, Part 15B Class A, CE, UL, IEC
10. Estandares: FCC Part 15B Class B
11. Puerto USB
12. Pantalla de LCD
13. Alimentación: 120/250 VAC
14. Fuente de poder doble
15. Topología de red: Full-NAT, Half-NAT, 802.1Q y otros
16. Funciones criptográficas: HTTPS, SSL
17. Administración vía HTTPS o SNMP o SSH.

4.3.5 Fase 3: Proceso de operación del servicio de sello de tiempo

El proceso del servicio de sello de tiempo se muestra en la TABLA Nº 4.8:

TABLA Nº 4.8: Proceso del servicio de sello de tiempo

N°	Descripción	Datos	Aplicativo	Condición de éxito
1	El usuario se auténtica mediante su certificado digital de autenticación.	Datos personales del usuario	Aplicativo de sello de tiempo	Recepción de datos de certificado digital
2	La SVA valida que la identidad del usuario.	Datos personales del usuario	Aplicativo de sello de tiempo	Identidad del usuario confirmada
3	La SVA verifica que existe un contrato vigente de servicios con el usuario.	Contrato de servicios	Aplicativo de sello de tiempo	Contrato de servicios vigente
4	A través de un canal https el usuario envía el archivo.	Certificado del usuario Archivo a firmar	Aplicativo de sello de tiempo	Documento
5	Servidor NTP valida su conexión con satélite	Identificación de satélite	Servidor NTP	Conexión validada
6	Servidor NTP identifica satélite con mejor señal y solicita fecha y hora exacta.	Identificación de satélite	Servidor NTP	Conexión establecida con satélite
7	Satélite establece comunicación segura con servidores Stratus 1.	Establece conexión segura	Satélite	Conexión establecida con servidor Stratus-1
8	Servidor Stratus-1 envía datos de fecha y hora exacta.	Envío de información	Servidor Stratus-1	Envío de información
9	Satélite re-trasmite información de fecha y hora exacta.	Recepción de información	Satélite	Re-trasmisión de información
10	Recepción de fecha y hora exacta.	Recepción de información	Servidor NTP	Recepción de datos de fecha y hora exacta
11	Agregar a documento los datos de fecha y hora exacta.	Documento integrado	Aplicativo de sello de tiempo	Archivo integrado con los datos de fecha y hora exacta

12	Firma digitalmente el archivo generado.	Documento integrado	Aplicativo de sello de tiempo	Archivo firmado digitalmente
13	Envío mediante aplicativo del archivo generado.	Documento integrado	Aplicativo de sello de tiempo	Archivo enviado
14	Envío de acuse de envío a correo electrónico del usuario.	Datos del usuario	Aplicativo de sello de tiempo	Acuse de recibo enviado
15	Recepción de acuse de recibo.	Datos de conformidad del servicio	Aplicativo de sello de tiempo	Recepción de acuse de recibo

Este proceso se puede observar mejor en la Fig. 4.4.

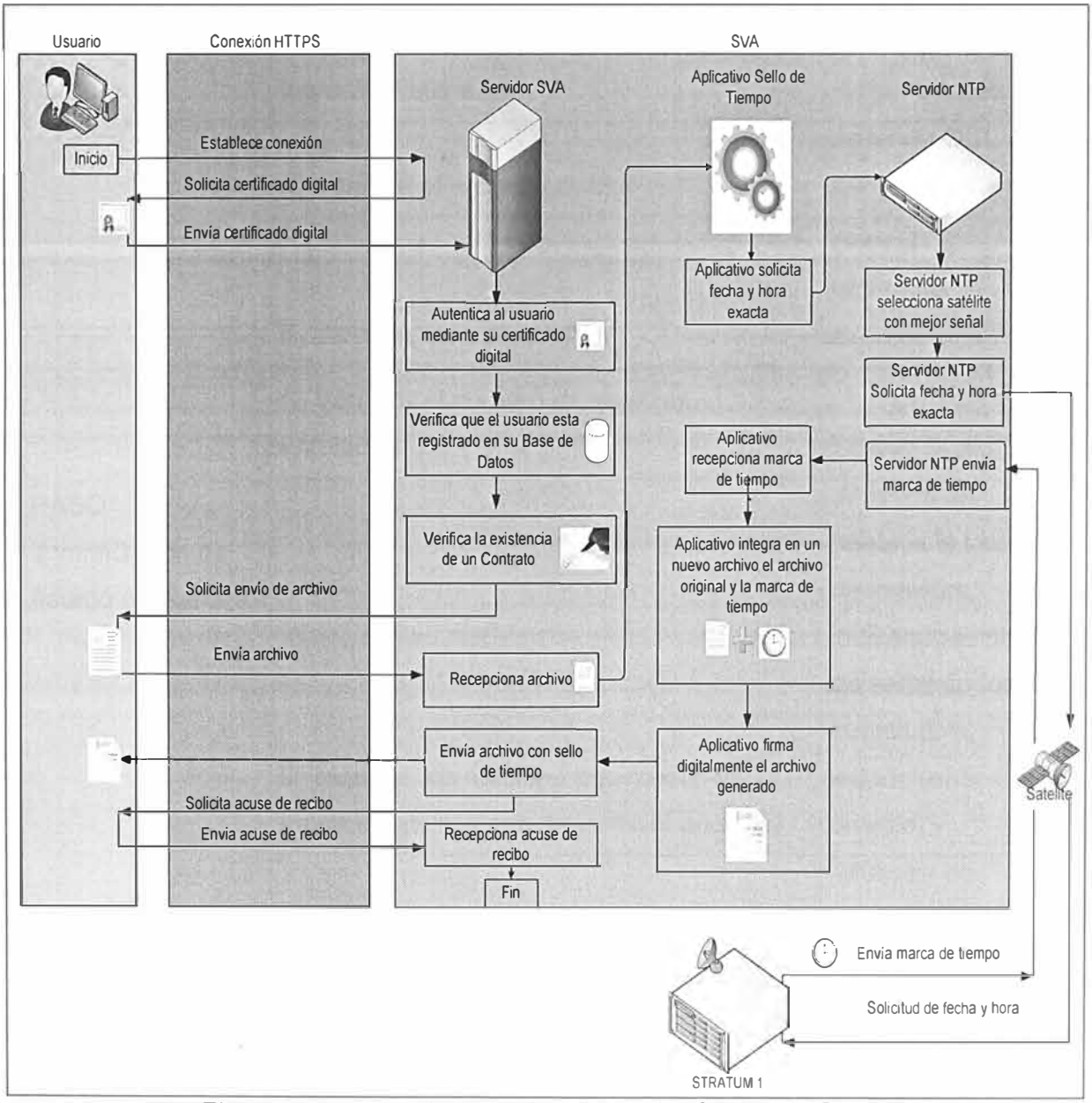


Fig. 4.4: Proceso de sello de tiempo del Centro de Datos

4.3.6 Proceso de verificación de servidor NTP

En la Tabla Nº 4.9, se describe la secuencia de pasos que se debe seguir para verificar el funcionamiento del servidor NTP.

Tabla Nº 4.9: Proceso de verificación de servidor NTP

SECUENCIA	DATOS	Resultados
PASO 1: ingresar al equipo vía telnet	A. Ingresar IP equipo NTP PRINCIPAL B. Ingresar IP equipo NTP CONTINGENCIA	Pantalla de bienvenida del servidor NTP
PASO 2:Autenticarse	A. Centro de datos principal	
	Ingresar usuario:	Ninguno
	Ingresar Password:	Login Successfull
	B. Centro de datos de contingencia	
	Ingresar usuario:	Ninguno -
	Ingresar Password:	Login Successfull
PASO 3:verificacion de estado del servicio	A. Verificar el enlace satelital	Antenna OK GPS: Locked
	B. Verificar hora de reloj	Hora UTC mostrada, sin zona horaria
	C. Verificar el numero de satélites enrolados	Survey Static,
	D. Mostrar los satélites localizados y mostrar satélites con mejor nivel de señal	Muestra en pantalla la Lista de satélites, indicando el nivel de señal de forma cuantitativa, estado (enable o disable)
	E. Mostrar ubicación del equipo	Muestra en pantalla la IP del equipo

4.3.7 Diseño de red de comunicaciones

Se presenta el siguiente diagrama de red (ver Fig. 4.4) diseñado bajo el cumplimiento de los criterios de alta disponibilidad, redundancia y balanceo de carga.

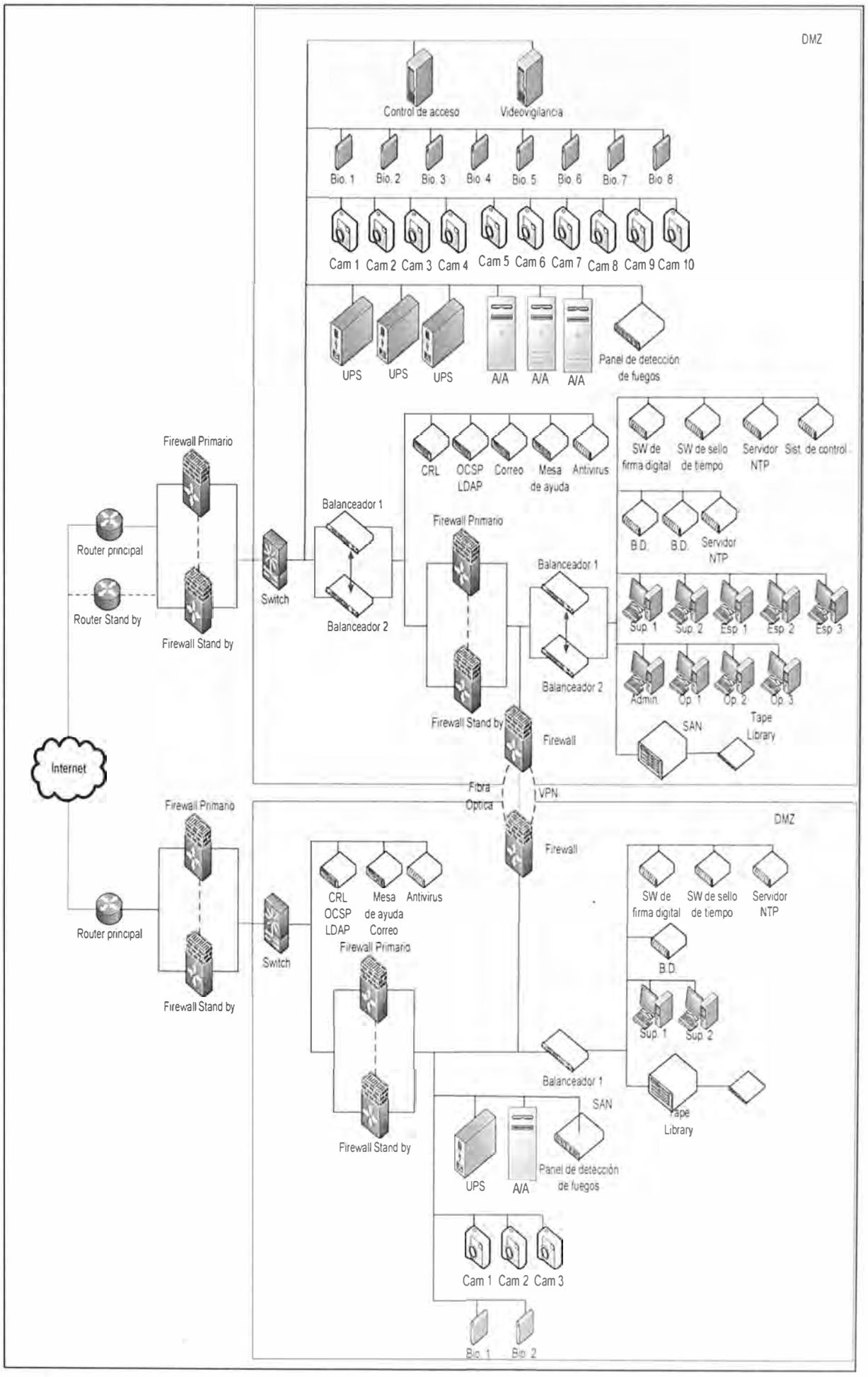


Fig. 4.5: Diseño de la estructura de red del Centro de Datos

4.3.8 Fase 4: Integración de dispositivos

Como parte de la integración de los dispositivos, se tienen que desarrollar la estructura de plan de pruebas (ver Tabla Nº 4.10), la cual se ha desarrollado de acuerdo a los criterios del BUILD SECURITY IN del Department of Homeland Security de los EEUU [33].

Tabla Nº 4.10: Estructura de plan de pruebas

N°	Nombre de la tarea
1	Identificación de dispositivos bajo pruebas
2	Identificación de Componentes de los dispositivos
3	Alcance de las pruebas
4	Limitaciones de las pruebas
5	Análisis de riesgo
6	Estrategia de las pruebas
7	Supuestos de inicio
8	Pruebas de aproximación
9	Activos que no van a ser objeto de prueba
10	Requerimientos para pruebas
11	Requerimientos para pruebas funcionales
12	Requerimientos para pruebas de seguridad
13	Requerimientos para pruebas de instalación/configuración
14	Requerimientos para pruebas de stress y carga
16	Personal requerido
17	Requerimientos de hardware e infraestructura
18	Pruebas de ambiente
19	Especificaciones de pruebas de caso
20	Identificadores de pruebas
21	Trazabilidad
22	Especificaciones de entrada/salida/Resultados esperados
23	Necesidades ambientales
24	Requerimientos de procedimientos especiales
25	Dependencia entre los casos de prueba
26	Automatización de las pruebas
27	Arquitectura de las pruebas automáticas
28	Herramientas de pruebas
29	Ejecución de las pruebas
30	Criterios de pruebas
31	Criterios de aceptación de pruebas
32	Pruebas de regresión
33	Procedimiento de pruebas
34	Cronograma de pruebas
35	Criterios de terminación de pruebas
36	Plan de Pruebas
37	Ejecución del Plan de Pruebas
38	Resultados de la ejecución del plan de pruebas
39	Registro de resultados Base de datos de conocimiento
40	Medidas correctivas a problemas encontrados

4.3.9 Fase 5: Planificación del proceso de acreditación

De acuerdo a la Tabla Nº 4.2, se tiene que elaborar un análisis de requerimientos contra la Guía de acreditación SVA, incluyendo:

- Anexo 1: Marco de la política de valor añadido
- Anexo 2: Reglamento de la ley de firmas y certificados digitales
- Anexo 3 Modelo de política de seguridad SVA
- Anexo 4: Controles del estándar ISO/IEC 17799
- y Anexos 5, 6, 7, 8, 9, 10 y 11 de la Guía de acreditación SVA.

El resultado de este análisis se muestra en la tabla Tabla Nº 4.11.

Tabla Nº 4.11 Análisis de requerimientos de la Guía de acreditación de la SVA

Referencia	Evidencia
ANEXO 1	
2.1. Comunidad de usuarios	VAPS (Declaración de Prácticas de Valor Añadido)
5. PUBLICACIÓN	VAPS del SVA. Política y Plan de Privacidad. Declaración de privacidad y seguridad. Contratos de tercerización.
6.1.2. Proceso de solicitud del certificado y responsabilidades	Contrato del usuario
7.1.1. Ubicación y construcción del local	Política de de Seguridad
7.1.7. Gestión de residuos	Política de gestión de residuos
7.1.8. Copia de seguridad externa	Procedimiento de copias de respaldo o de seguridad externa de toda la información sensible.
7.3. Controles de personal	Política de Privacidad
7.3.2. Procedimiento para verificación de antecedentes	Procedimientos para la verificación de antecedentes.
7.3.3. Requisitos de capacitación	Programa de capacitaciones al personal
7.3.5. Frecuencia y secuencia de la rotación en el trabajo	Política de rotación en el trabajo
7.3.6. Sanciones por acciones no autorizadas	Proceso disciplinario ante faltas
7.4.1. Tipos de eventos registrados	Registros de auditorías de eventos
7.4.2. Frecuencia del procesamiento del registro	Procedimiento de análisis de auditoría.
7.4.4. Protección de registro de auditorías	Plan de Seguridad
7.4.5. Procedimiento de copia de seguridad del registro de auditorías	Proceso de copia de seguridad del registro de auditorías.
7.5.2. Periodo de conservación del archivo	Proceso de copia de seguridad del registro de auditorías.
7.5.3. Protección del archivo	Política de Seguridad.

7.5.4. Procedimientos para copia de seguridad del archivo	Proceso de copia de seguridad de información y software esencial.
7.5.5. Requisitos para los archivos de sellado de tiempo	Proceso de sellado de tiempo deben consignar la fecha y hora, y la firma digital dela organización que genera dichos datos según la RFC 3161 (Time Stamping).
7.5.6. Procedimiento para obtener y verificar la información del archivo	Plan de Privacidad
7.6. Recuperación frente al compromiso y desastre	Plan de contingencias
8.2. Estándares y controles para el módulo criptográfico	Certificado de cumplimiento de los módulos criptográficos de FIPS 140-2 nivel de seguridad 2 o Common Criteria EAL 4+, como mínimo.
8.4.1. Controles de desarrollo del sistema	Certificado de acreditación del software ante INDECOPI.
8.4.3. Evaluación de seguridad del ciclo de vida	Auditorías de seguridad
8.5. Controles de seguridad de la red	Auditorías de seguridad
8.6. Sello de tiempo	Se admiten servicios de sellado de hora y tiempo según la norma ISO/IEC 18014-1:2000 . Empleo de fuente confiable de tiempo.
10.2. Confidencialidad de la información del negocio	Acuerdo de confidencialidad
10.4.2. Política y Plan de privacidad	Política de Privacidad Plan de Privacidad
10.6.1. Cobertura de seguro	Seguro por un monto mínimo de $ 35 000.00 dólares americanos.
10.11. Provisiones sobre resolución de disputas	Procedimientos de resolución de disputas
ANEXO 2	
Política de Seguridad	Política de Seguridad
Valoración de riesgos	Informe Auditor Independiente.
Plan de Continuidad del Negocio.	Plan de Continuidad del Negocio.
Plan de Recuperación de Desastres.	Plan de Recuperación de Desastres.
Plan de Seguridad del Sistema de Información. Plan de Administración de Claves	Informe Auditor Independiente. Informe Auditor Independiente.
Documento de Cumplimiento de Estándares Tecnológicos.	Informe Auditor Independiente. Manuales de los fabricantes de hardware Manuales de los fabricantes de software

	Documento de Cumplimiento de Estándares Tecnológicos.
Plan de Seguridad Física y Ambiental.	Informe Auditor Independiente.
Documento de evaluación de personal.	Informe Auditor Independiente.
Documento de Evaluación del Oficial de Seguridad.	Informe Auditor Independiente.
ANEXO 9	
Memoria descriptiva y funcionan	Memoria descriptiva y funcional
ANEXO 10	
Ficha de solicitud de acreditación como prestador de servicios de valor añadido (SVA)	Ficha de solicitud de acreditación como prestador de servicios de valor
ANEXO 11	
Documento de cumplimiento de los requerimientos de Usabilidad	Documento de cumplimiento de los requerimientos de Usabilidad

4.3.10 Fase 6: Ejecución del plan de acreditación

De lo analizado, para el proceso de acreditación se debe elaborar, implementar, obtener, etc. los documentos indicados en la Tabla Nº 4.11.

Para la ejecución del plan de acreditación se debe precisar a los responsables de la consecución de los requerimientos, así como las acciones requeridas para las mismas de acuerdo a la siguiente:

Tabla Nº 4.12: Responsables de los requerimientos de acreditación

Requerimientos	Acción	Responsable
VAPS (Declaración de Prácticas de Valor Añadido)	Elaboración Interna	Personal del Centro de Datos
VAPS del SVA.	Elaboración Interna	Personal del Centro de Datos
Política de Privacidad.	Elaboración Interna	Departamento Legal
Plan de Privacidad.	Elaboración Interna	Departamento Legal
Declaración de privacidad	Elaboración Interna	Departamento Legal
Declaración de seguridad.	Elaboración Interna	Departamento de Seguridad de la Información
Contratos de tercerización.	Elaboración Interna	Departamento Legal
Contrato del usuario	Elaboración Interna	Departamento Legal
Política de gestión de residuos	Elaboración Interna	Personal del Centro de Datos

Procedimiento de copias de respaldo o de seguridad externa de toda la información sensible.	Elaboración Interna	Personal del Centro de Datos
Política de Privacidad	Elaboración Interna	Personal del Centro de Datos
Procedimientos para la verificación de antecedentes.	Elaboración Interna	Departamento de Seguridad de la Información
Programa de capacitaciones al personal	Elaboración Interna	Departamento de Recursos Humanos
Política de rotación en el trabajo	Elaboración Interna	Departamento de Recursos Humanos
Proceso disciplinario ante faltas	Elaboración Interna	Departamento de Recursos Humanos
Registros de auditorías de eventos	Recopilación de información durante un tiempo establecido	Personal del Centro de Datos
Procedimiento de análisis de auditoría.		Departamento de Seguridad de la Información
Plan de Seguridad	Elaboración Interna	Departamento de Seguridad de la Información
Proceso de copia de seguridad del registro de auditorías.	Elaboración Interna	Personal del Centro de Datos
Política de Seguridad.	Elaboración Interna	Departamento de Seguridad de la Información
Proceso de copia de seguridad de información y software esencial.	Elaboración Interna	Personal del Centro de Datos
Proceso de sellado de tiempo	Elaboración Interna	Personal del Centro de Datos

Plan de Privacidad	Elaboración Interna	Responsable de privacidad
Plan de contingencias	Elaboración Interna	Personal del Centro de Datos Departamento de Seguridad de la Información
Certificado de cumplimiento de los módulos criptográficos de FIPS 140-2 nivel de seguridad 2 o Common Criteria EAL 4+, como mínimo.	Documentación del fabricante	Departamento de Seguridad de la Información
Certificado de acreditación del software ante INDECOPI.	Certificado emitido por INDECOPI	Consultora externa
Auditorías de seguridad	Procedimiento interno	Departamento de Seguridad de la Información
Se admiten servicios de sellado de hora y tiempo según la norma ISO/IEC 18014-1:2000 . Empleo de fuente confiable de tiempo.	Implementación del servicio de sello de tiempo	Personal del Centro de Datos
Acuerdo de confidencialidad	Elaboración interna	Departamento Legal
Política de Privacidad	Elaboración interna	Responsable de privacidad
Plan de Privacidad	Elaboración interna	Responsable de privacidad
Seguro por un monto mínimo de $ 35 000.00 dólares americanos.	Contratación externa	Servicio externo
Procedimientos de resolución de disputas	Elaboración interna	Departamento Legal
Política de Seguridad	Elaboración interna	Departamento de Seguridad de la Información
Plan de Continuidad del	Elaboración interna	Departamento de

Negocio.		Seguridad de la Información
Plan de Recuperación de Desastres.	Elaboración interna	Departamento de Seguridad de la Información
Valoración de riesgos	Consultoría externa	Consultoría externa
Manuales de los fabricantes de hardware	Documentación del fabricante	Departamento de Seguridad de la Información
Manuales de los fabricantes de software	Documentación del fabricante	Departamento de Seguridad de la Información
Documento de Cumplimiento de Estándares Tecnológicos.	Recopilación de información	Consultoría externa
Memoria descriptiva y funcional	Elaboración interna	Departamento de Seguridad de la Información
Ficha de solicitud de acreditación como prestador de servicios de valor	Elaboración interna	Departamento de Seguridad de la Información
Documento de cumplimiento de los requerimientos de Usabilidad	Elaboración interna	Departamento de Usabilidad
Plan de Seguridad del Sistema de Información.	Elaboración interna	Consultoría externa
Plan de Administración de Claves	Elaboración interna	Consultoría externa
Plan de Seguridad Física y Ambiental.	Elaboración interna	Consultoría externa
Documento de evaluación de personal.	Elaboración interna	Consultoría externa
Documento de Evaluación del Oficial de Seguridad.	Elaboración interna	Consultoría externa

El proceso de acreditación (de acuerdo a INDECOPI) como SVA de sello de tiempo tiene tres fases:

- FASE I: Evaluación preliminar de la solicitud y expediente de acreditación
- FASE II: Evaluación de la capacidad tecnológica instalada del SVA solicitante. Esta evaluación Consta de 2 pasos y a su vez cada uno de los pasos cuenta, de ser necesaria, con su respectiva Evaluación Complementaria:
- FASE III: Decisión: Corresponde al INDECOPI emitir decisión en relación a la procedencia o no de la acreditación de la SVA Solicitante

Estas fases se detallan mejor en la Tabla Nº 4.13:

Tabla Nº 4.13: Proceso de acreditación de SVA como servicio de sello de tiempo

FASE	Pasos	Tiempo	Documentación	Condición	Salida
FASE I	Paso1: Evaluación preliminar	Plazo: 5 días	Resolución de admisibilidad	Se declara conformidad de documentación y se cita al representante técnico de SVA solicitante.	La SVA solicitante de la acreditación de Sello de Tiempo pasa a la Fase II:
			Informe de comité evaluador	Improcedencia no levantada de la Solicitud	Conclusión del Procedimiento
FASE II	Paso 1: Evaluación de: Declaración de prácticas de valor añadido Política de privacidad Plan de privacidad Política de seguridad Requerimientos de usabilidad.	La SVA solicitante cuenta con un plazo de 5 días para presentar la propuesta de acciones correctivas	Informe de comité evaluador	Ausencia no conformidades	Continúa la Fase II: Evaluación De Interoperabilidad
			Informe de comité evaluador	No conformidades presentes	Inicio a la Evaluación Complementaria
	Evaluación complementaria	Plazo: 5 días	Acta de comité evaluador		Continúa la Fase II: Evaluación De Interoperabilidad
	Paso 2. Evaluación de Interoperabilidad	**No hay tiempo fijado**	Pruebas de TSL	Ausencia de no conformidades	Continúa la Fase III: DECISION.

				No conformidades presentes	Inicio a la Evaluación Complementaria
FASE III	Decisión	**No hay tiempo fijado**	Inscripción en Lista TSL	Otorga la acreditación al SVA solicitante.	SVA acreditada ingresa a la IOFE. FIN del proceso
				Deniega la Acreditación	Pase a fase de RECLAMOS
	Reclamos	Plazo: 5 días	Recurso impugnatorio por parte del solicitante	Resolución de INDECOPI.	Retorno a fase de Decisión

CAPITULO V
COSTOS DEL PROYECTO

En este capítulo de muestran los costos relacionados al servicio de sello de tiempo (ver Tabla Nº 5.1) y también para el proceso de acreditación ante INDECOPI como SVA de sello de tiempo. Se va a utilizar las siguientes nomenclaturas:

- Supervisor de Operaciones: SO
- Ingeniero de Operaciones: IO
- Administrador de Red: AR
- Administrador de base de datos: AB
- Desarrollador de aplicaciones: DA
- Oficial de seguridad: OS
- Supervisor de servicios: SS
- Coordinador de seguridad 1: CS1
- Coordinador de seguridad 2: CS2
- Administrador de mesa de ayuda: AM
- Operador de mesa de ayuda 1: OM1
- Operador de mesa de ayuda 2: OM2
- Operador de mesa de ayuda 3: OM3
- Jefe de Centro de Datos: JC
- Consultora externa: CE
- Servicio externo: SE

Tabla Nº 5.1: Costos asociados al proyecto

N°	Concepto	Tipo de gasto	Rubro	Personas	Cantidad	Horas	Costo (USD)	Costo Total
1	Consultoría para la ejecución de Ethical Hacking	CAPEX	Consultoría	CE	1	N/A	5000	5000
2	Servicio de traslado y custodia de activos de información	CAPEX	Servicio	SE	1	N/A	20000	20000

3	Consultoría para la acreditación como SVA ante INDECOPI, incluye: •Auditoria externa de cumplimiento •Levantamiento de observaciones •Obtención de acreditación	CAPEX	Consultoría	CE	1	N/A	30000	30000
4	Elaboración de especificaciones técnicas	OPEX	CAS	SO	1	40	14	560
5	Compra de equipos: Firewall internos (04 unidades)	CAPEX	Dispositivo	SE	1	N/A	13000	52000
6	Compra de equipos: Firewall externos (04 unidades)	CAPEX	Dispositivo	SE	1	N/A	13000	52000
7	Compra de equipos: Servidor NTP (03 unidades)	CAPEX	Dispositivo	SE	1	N/A	7000	21000
8	Compra de equipos: Balanceador de carga (05 unidades)	CAPEX	Dispositivo	SE	1	N/A	18000	90000
9	Servicio de instalación y configuración de equipos: •Firewall (08 unidades) •Servidor NTP (03 unidades) •Balanceador de carga (05 unidades) •Pruebas de funcionamiento	CAPEX	Dispositivo	SE	1	N/A	20000	20000

10	Elaboración de Plan de pruebas	OPEX	CAS	SO IO AR AB DA	5	56	14	3920
11	Ejecución de Plan de Pruebas, incluye: •Pruebas al centro de datos principal •Pruebas al centro de datos de contingencia •Pruebas de funcionamiento del servicio de sello de tiempo	OPEX	CAS	SO IO AR AB DA	5	240	14	16800
12	Auditoría interna Alcance: •Centro de Datos Principal •Centro de Datos de Contingencia Incluye: •Auditoria •Levantamiento de no conformidades	OPEX	CAS	OF JC IO SO IO AR DB DA	8	40	14	4480
				SS CS1 CS2	3	40	10	1200
				AM	1	40	8	320
				OM1 OM2 OM3	3	40	7	840

13	Elaboración de documentación del Expediente de Acreditación de la SVA	OPEX	CAS	OS IO	2	168	14	4704
				SS CS1 CS2	3	168	10	5040
				AM	1	168	8	1344
					CAPEX			**290000**
					OPEX			**39208**
					TOTAL			**329208**

CONCLUSIONES Y RECOMENDACIONES

Las conclusiones obtenidas en el presente informe son las siguientes:

1. El servicio de sello de tiempo garantiza de manera segura y sin lugar a dudas la existencia de conjunto de datos (archivos digitales) desde un fecha y hora única y que ninguno de estos datos ha sido modificado desde entonces.
2. El servicio de sello de tiempo, utilizando la firma digital, certificado digital, clave pública y clave privada, garantizan la seguridad en las transacciones electrónicas.
3. Para brindar el servicio de sello de tiempo y que este servicio tenga valor legal dentro del territorio nacional se debe seguir un proceso de acreditación ante INDECOPI como Servicio de Valor Agregado (SVA).
4. Para poder brindar el servicio de sello de tiempo con criterios de alta disponibilidad, redundancia y balanceo de carga, es necesario contar con una red de comunicaciones basadas en hardware, en este informe se ha identificado que estos dispositivos son firewalls, balanceadores de carga y servidores NTP, además se ha realizado un análisis detallado para determinar las características que estos deben cumplir para satisfacer los criterios indicados.

ANEXO A
GLOSARIO

- AUTORIDAD ADMINISTRATIVA COMPETENTE(AAC): Organismo público responsable de acreditar a las Entidades de Certificación, a las Entidades de Registro o Verificación y a los Prestadores de Servicios de Valor Añadido, públicos y privados, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica y de supervisar dicha infraestructura. Dicha responsabilidad recae en el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual- INDECOPI.
- ER: Entidad de Registro o Verificación, acreditada por la Autoridad Administrativa Competente, la cual estará encargada del levantamiento de datos, comprobación de la información del solicitante, identificación y autenticación de los titulares y Suscriptores, aceptación y autorización de solicitudes de emisión, cancelación, modificación, re-emisión y suspensión de Certificados Digitales.
- EC: Entidad de Certificación, acreditada por la Autoridad Administrativa Competente, que estará encargada de proporcionar, emitir o cancelar los Certificados Digitales, a personas naturales y jurídicas, así como a funcionarios, empleados y servidores públicos, para el ejercicio de sus funciones y la realización de actos de administración interna e interinstitucional y a las personas expresamente autorizadas por la entidad pública correspondiente.
- MEDIO ELECTRÓNICO SEGURO: medios electrónicos que emplean firmas y certificados digitales emitidos por Prestadores de Servicios de Certificados Digital acreditados, donde el intercambio de información se realiza a través de canales seguros.
- POLÍTICA DE SEGURIDAD: Una política de seguridad es el resultado de la elaboración de un conjunto de documentos basados en el estudio de la estructura del negocio, la que encuentra basada en términos que garanticen la seguridad de los procesos de registro en la Entidad de Registro.
- PLAN DE PRIVACIDAD: El plan de privacidad debe establecer el tipo de datos personales que pueden ser recolectados y cómo serán utilizados, protegidos, recuperados/corregidos, circunstancias en que estos serán revelados y las sanciones en caso de incumplimiento del plan.
- TSL: La Lista de Servicio de Confianza (TSL) contiene los nombres y, en varios casos los certificados digitales raíces de las Entidades Prestadoras de Servicios de Certificación Digital (PSCs), consideradas de confianza. La inscripción de una SVA en la TSL significa que ésta se encuentra acreditada por la Autoridad Administrativa competente (Indecopi), conforme al Reglamento de la Ley de Firmas y Certificados Digitales, aprobado por Decreto Supremo 052-2008-PCM. La Lista en sí misma es firmada digitalmente por el Indecopi.

- VAPS: Documento oficialmente presentado por una Prestadora de Servicios de valor Añadido a la Autoridad Administrativa Competente, contiene la declaración de los procedimientos, procesos, métodos, etc. que utiliza esta para brindar el servicio de sello de tiempo.

ANEXO B
FUENTE DE FIGURAS Y TABLAS

BIBLIOGRAFÍA

[1] Everis / CELA-IESE Business School, http://www.everis.com/spain/WCRepositoryFiles/110494%20CELA%20JUNIO%202011%20WEB.pdf

[2] Instituto de Opinión Publica de la PUCP, http://iop.pucp.edu.pe/images/documentos/Uso%20de%20Internet%20Junio%202010%20(nacional).pdf

[3] INDECOPI,http://www.indecopi.gob.pe/0/modulos/JER/JER_Interna.aspx?ARE=0&PFL=6&JER=440

[4] Portal de servicios al ciudadano, http://www.serviciosalciudadano.gob.pe/

[5] APEC http://www.apec.org/Meeting-Papers/Ministerial-Statements/Mining/2005_mining.aspx

[6] HISPASEC, http://www.hispasec.com/unaaldia/322

[7] Network Time Synchronization Research Project: http://www.eecis.udel.edu/~mills/ntp.html

[8] Network Time Protocol, http://www.ntp.org/

[9] Introduction to NTP, http://www.akadia.com/services/ntp_synchronize.html

[10] David L. Mills, "Computer Network Time Synchronization: The Network Time Protocol", Universidad de Delaware-EEUU, 2006.

[11] Peter Rybaczyk, "Expert Network Time Protocol: An Experience in Time with NTP" Appress- EEUU, 2005

[12] Cisco, https://learningnetwork.cisco.com/docs/DOC-8774

[13] Modelo OSI, http://www.vlsm-calc.net/models.php?lang=en

[14] Alta disponibilidad en Linux, http://www.ibiblio.org/pub/linux/docs/LuCaS/Presentaciones/200103hispalinux/paredes/pdf/LinuxHA.pdf

[15] ANSI/TIA942 Telecommunications Infrastructure Standard for Data Centers, http://informatica.iessanclemente.net/manuais/images/9/9f/Tia942.pdf

[16] Alfonso Garcia-Cervigon Hurtado, "Seguridad Informática", Paraninfo, 2011

[17] INDECOPI, "Guías de acreditación SVA", Perú, 2007

[18] Premio Proyectos 2012 Cumbre Mundial de la Sociedad de la Información CMSI http://groups.itu.int/stocktaking/WSISProjectPrizes2012.aspx#voteTab

[19] All internet Security, http://www.all-internet-security.com/top_10_firewall_software.html

[20] Zone Alarm PRO Firewall, http://www.zonealarm.com/security/de/zonealarm-pro-firewall-anti-spyware.htm

[21] Panda Global Protection 2012, http://www.pandasecurity.com/homeusers/solutions/global-protection/

[22] FORTINET 310B, http://www.fortinet.com/products/fortigate/310B.html

[23] JUNIPER IDP75, http://www.juniper.net/us/en/local/pdf/datasheets/1000221-en.pdf

[24] Check Point 2200,http://www.checkpoint.com/products/2000-appliances/

[25] Symmetricom NTP 150, http://www.symmetricom.com/products/ntp-servers/ntp-network-appliances/?i=6097

[26] LANTIME M300/GPS, http://www.meinberg.de/english/products/lantime-m300-gps.htm

[27] NTS-6001, http://www.galsys.co.uk/ntp-servers/nts-6001-gps-ntp-server.html

[28] Tempus LX GPS, http://www.endruntechnologies.com/pdf/TempusLxGPS.pdf

[29] Radware APP 2016 http://www.radware.com/Products/ApplicationDelivery/AppDirector/default_TechSpec.aspx

[30] BIG-IP 8950, http://www.f5.com/pdf/products/big-ip-platforms-ds.pdf

[31] Barracuda 640, http://www.barracudanetworks.com/ns/downloads/Datasheets/Barracuda_Load_Balancer_DS_ES.pdf

[32] Coyote Point E650GX, http://www.coyotepoint.com/products/e650gx

[33] Department of Homeland Security, https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/testing/255-BSI.pdf