

**ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**

**FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN**

INFORME DE MATERIA DE GRADUACION

“ANÁLISIS, DETECCIÓN Y SOLUCIÓN AL GRADO DE EXPOSICION DE VULNERABILIDADES EN SERVIDORES LINUX PARA LA INSTITUCIÓN FINANCIERA **DROFMAN**”

**TESINA DE SEMINARIO**

Previa la obtención del Título de:

**LICENCIADA(O) EN REDES Y SISTEMAS OPERATIVOS**

Presentada por:

**EDUARDO JAVIER LOOR ALCÍVAR**

**SANDRA CATHERINE VÁSQUEZ MITE**

GUAYAQUIL – ECUADOR

AÑO 2013

AGRADECIMIENTO

A Dios sobre todas las cosas, por permitirnos culminar de manera satisfactoria nuestros estudios y llevarnos a cumplir una de nuestras metas.

A la familia, por ser nuestra guía de formación humana, por darnos la educación y principios, que nos llevan a ser la persona que somos hoy.

A nuestros profesores y a todas las personas que nos apoyaron en el desarrollo de este trabajo.

Y a todos quienes fomentan el desarrollo tecnológico en Ecuador.

DEDICATORIA

A Dios por la fortaleza que nos ha brindado al realizar este trabajo, por su infinito amor reflejado en nuestros seres queridos y maestros.

A nuestros padres y seres queridos por su comprensión y apoyo incondicional, quienes siempre fomentaron diligencia y perseverancia con valores éticos, y que nunca nos dejaron decaer ni darnos por vencidos.

# DECLARACION EXPRESA

“La responsabilidad del contenido de este Trabajo de Grado, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral”

(Reglamento de Graduación de la ESPOL)

|  |
| --- |
| Eduardo Javier Loor Alcívar |
| Sandra Catherine Vásquez Mite |

# TRIBUNAL DE SUSTENTACIÓN

Ing. Fabián Barboza

Profesor de Seminario de Graduación

Ing.

Delegado del Decano

RESUMEN

El principal objetivo de este proyecto es implementar la metodología aprendida en nuestro desarrollo académico y en el seminario asistido con respecto a “LINUX NETWORKING Y SEGURIDADES”**,** para fortalecer la seguridad informática en servidores para instituciones financieras aplicado a la empresa “DROFMAN S.A.” la cual ha solicitado un estudio de su infraestructura TI, detectando vulnerabilidades, aplicando soluciones e implementar un plan de prevención a futuro para mitigar los riesgos de seguridad y cumplir con los requerimientos del Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS).

INDICE

**INTRODUCCIÓN**

El objetivo del proyecto es fortalecer la seguridad informática en servidores para instituciones financieras aplicando nuestros conocimientos y demás temas aprendidos durante el trascurso de la materia de graduación.

En el primer capítulo, haremos una descripción detallada de conceptos sobre el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS) para una mejor comprensión de lo que debe cumplir la empresa.

En el segundo capítulo se menciona el análisis de la infraestructura TI de la empresa, detallando su distribución y la tecnología aplicada en el manejo de información de tarjetas de crédito a la cual le aplicaremos nuestro proyecto.

En el tercer capítulo, se da un detalle sobre la identificación de las vulnerabilidades existentes tras el análisis de la Infraestructura TI de la empresa, su clasificación y la matriz de impacto en el negocio.

El cuarto y último capítulo se muestra la implementación de las soluciones en servidores de desarrollo, el análisis de resultados de las pruebas para luego aplicarlas a PRE-PRODUCCION y posterior en Producción para al final implementar un plan de prevención contra vulnerabilidades.

**CAPITULO 1:**

**ESTANDAR PCI-DSS**

**Introducción**

El **Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago** (PCI DSS), fue desarrollado por un comité conformado por la compañías más importantes de tarjetas denominado **Payment Card Industry Security Standards Council** (PCI SSC), como una guía para organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes, asegurando su infraestructura de TI para garantizar que la información de sus clientes este totalmente protegida y cifrada.

**Qué es PCI-DSS?**

El **Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago** (PCI-DSS), es un conjunto de directrices de prácticas de seguridad de red y empresariales que deben ser observados y aplicados con la finalidad de garantizar la seguridad de la información, disminuyendo el riesgo de compromiso de esta información mediante un manejo adecuado de los datos de las tarjetas de pago.

El **Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago** (PCI-DSS), es además un acuerdo contractual que describe en detalle cómo deben ser manejados los datos sensibles de las tarjetas de pago. La norma describe claramente lo que debe hacer en forma de “Cumplimiento de Requisitos” y la forma de demostrarlo en forma de “Requerimientos de validación”.

**Requerimientos de PCI DSS**

Los 12 requerimientos del Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago **(PCI DSS)** son un conjunto de controles de seguridad que las empresas están obligadas a implementar para proteger los datos de las tarjetas de crédito y cumplir con el Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS). Los requerimientos han sido desarrollados y mantenidos por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI).

Cualquier organización que reciba tarjetas de pago, incluyendo tarjetas de débito y crédito, deberá cumplir con los 12 requerimientos de forma directa o bien a través de un control de compensación. No obstante, los controles de compensación no siempre se admiten y deben ser aprobados bajo un criterio de caso, por parte de un asesor de seguridad cualificado de la PCI (QSA PCI).

Los 12 requerimientos de las PCI DSS **(Tabla1).**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Principios** | | | | **Requerimientos** | | | | | | |
| Construir y mantener una red segura | | | | Requerimiento 1: Instalar y mantener un cortafuego y su configuración para proteger la información de tarjetas. | | | | | | |
| Requerimiento 2: No emplear parámetros de seguridad y usuarios del sistema por defecto. | | | | | | |
| Proteger los datos de tarjetas | | | | Requerimiento 3: Proteger los datos almacenados de tarjetas. | | | | | | |
| Requerimiento 4: Cifrar las transmisiones de datos de tarjetas en redes abiertas o públicas. | | | | | | |
| Mantener un programa de gestión de Vulnerabilidades | | | | Requerimiento 5: Usar y actualizar regularmente software antivirus. | | | | | | |
| Requerimiento 6: Desarrollar y mantener de forma segura sistemas y aplicaciones. | | | | | | |
| Implementar medidas de control de acceso | | | | Requerimiento 7: Restringir acceso a la información de tarjetas según "need-to-know". | | | | | | |
| Requerimiento 8: Asignar un único ID a cada persona con acceso a computadoras. | | | | | | |
| Requerimiento 9: Restringir acceso físico a la información de tarjetas. | | | | | | |
| Monitorizar y testear regularmente las Redes | | | | Requerimiento 10: Auditar y monitorizar todos los accesos a los recursos de red y datos de tarjetas. | | | | | | |
| Requerimiento 11: Testear de forma regular la seguridad de los sistemas y procesos. | | | | | | |
| Mantener una política de seguridad de la Información | | | | Requerimiento 12: Mantener una política que gestione la seguridad  de la información. | | | | | | |
|  |  |  |  |  |  |  |  |  | **(Tabla 1)** |
|  |  |  |  |  |  |  |  |  |  |

**Por qué se debe cumplir PCI DSS**

Una organización puede buscar cumplir con el Estándar de seguridad de datos de la Industria de Tarjetas de Pago por varias razones.

Frecuentemente, dicho requerimiento se origina de una fuente externa; el volumen de transacciones que procesa o bien debido a un incidente de seguridad.

Algunas organizaciones y/o compañías financieras progresistas buscan cumplir con el estándar porque desde el punto de vista de sus negocios no desean estar asociadas a ningún hurto virtual, que no es otra cosa que el fraude electrónico a través de tarjetas de crédito. El cumplimiento con la norma PCI DSS permite a una organización y/o compañía financiera reducir considerablemente su exposición a los riesgos.

**Como cumplir PCI DSS**

Los comerciantes y otras entidades que almacenan, procesan y/o transmiten datos de tarjetahabientes deben cumplir con PCI DSS. Si bien el Consejo es responsable de la gestión de las normas de seguridad de datos, cada marca de tarjetas de pago mantiene sus propios programas independientes de aplicación de conformidad.

Cada marca de tarjetas de pago ha definido los requisitos específicos para la validación de cumplimiento y presentación de informes, tales como las disposiciones para la realización de autoevaluaciones y el momento de contratar a un QSA. Dependiendo de la clasificación de la entidad o el nivel (determinado por las distintas marcas de tarjetas de pago) riesgo, los procesos de validación de cumplimiento y presentación de informes a la adquisición de instituciones financieras suelen seguir esta pista:

1. **Definición del alcance de PCI DSS.-** Determinar qué componentes del sistema se rigen por PCI DSS.
2. **Evaluación.-** Examinar la conformidad de los componentes del sistema de alcance.
3. **Controles de compensación**.- Asesorar alternativas de control de tecnología y/o procesos válidos.
4. **Informes.-** Presentar la documentación requerida por el asesor y/o entidad.
5. **Justificaciones.-**  Aclarar o actualizar reportes de informes si aplican a petición de la entidad adquiriente o la marca de tarjetas de pagos.

Las preguntas específicas sobre niveles de validación de cumplimiento deben dirigirse a su entidad financiera, la adquisición o la marca de tarjetas de pago. Sólo la entidad financiera adquiriente puede asignar un nivel de validación para los comerciantes.

**Selección de un Asesor de Seguridad Calificado**  
Un asesor de seguridad cualificado (QSA) es una empresa de seguridad de datos que se ha formado y está certificado por el Consejo de Estándares de Seguridad (PCI) para llevar a cabo evaluaciones de la seguridad en el lugar, para verificar el cumplimiento con PCI DSS. El QSA hará lo siguiente:

* Verificar toda la información técnica proporcionada por comercio o proveedor de servicios.
* Utilizar un juicio independiente para confirmar que el estándar se ha cumplido.
* Proporcionar apoyo y orientación durante el proceso de cumplimiento.
* Estar en el lugar para la validación de la evaluación o la duración según sea necesario.
* Revisar el producto de trabajo que soporte los requisitos de PCI DSS y su evaluación de los procedimientos de seguridad.
* Asegurarse de que la adhesión a los Procedimientos de Evaluación de Seguridad (PCI DSS)
* Validar el alcance de la evaluación.
* Selección de los sistemas y componentes del sistema que se emplean en el muestreo.
* Evaluar los controles de compensación.
* Elaborar el informe final.

El QSA seleccionado debe tener conocimientos sólidos del negocio y tener experiencia en la evaluación de la seguridad de las organizaciones similares. Ese conocimiento ayuda al QSA a entender los matices de negocio específicos por sector de seguridad de los datos de tarjetahabientes bajo PCI DSS. Por otra parte, buscar un buen ajuste con la cultura de su empresa. La evaluación concluirá si se cumplen o no, pero el QSA también trabajará con su organización para ayudar a entender cómo lograr y mantener el cumplimiento de la misma. Muchos QSA también pueden proporcionar servicios adicionales relacionados con la seguridad, tales como la evaluación de las vulnerabilidades actuales y remediación de las mismas.

**Ámbito de la evaluación del cumplimiento**

El proceso de determinación del alcance incluye la identificación de todos los componentes del sistema que se encuentran dentro o conectados al entorno de datos de titulares de tarjetas. El entorno del titular se compone de personas, procesos y tecnología que manejan datos de los tarjetahabientes o datos confidenciales de autenticación. Los componentes del sistema incluyen dispositivos de red (cable e inalámbricas), servidores y aplicaciones. Componentes de virtualización, tales como máquinas virtuales, switches, routers, dispositivos virtuales, aplicaciones virtuales, desktops, e HyperV, también se consideran los componentes del sistema dentro de PCI DSS.

Las entidades deben confirmar la exactitud e idoneidad del alcance PCI DSS mediante la realización de los siguientes pasos:

* La entidad evaluada identifica y documenta la existencia de todos los datos de los titulares de su entorno, para comprobar que no existen datos de los tarjetahabientes fuera del entorno del titular actualmente definido (CDE).
* Una vez que todas las ubicaciones de los datos de los tarjetahabientes son identificados y documentados, la entidad utiliza los resultados para comprobar que el alcance de PCI DSS es apropiado (por ejemplo, los resultados pueden ser un diagrama o un inventario de ubicaciones de datos de titulares de tarjetas).
* La entidad considera los datos de titulares de tarjetas que se encuentren en el ámbito de la evaluación de PCI DSS y parte de la CDE a menos que tales datos se eliminan o migraron/consolidaron en el CDE definida actualmente.
* La entidad retiene la documentación que muestra cómo se confirmó el alcance de PCI DSS y los resultados, para su examen evaluador y/o de referencia durante la próxima actividad confirmación alcance SCC PCI anual.

**CAPITULO 2:**

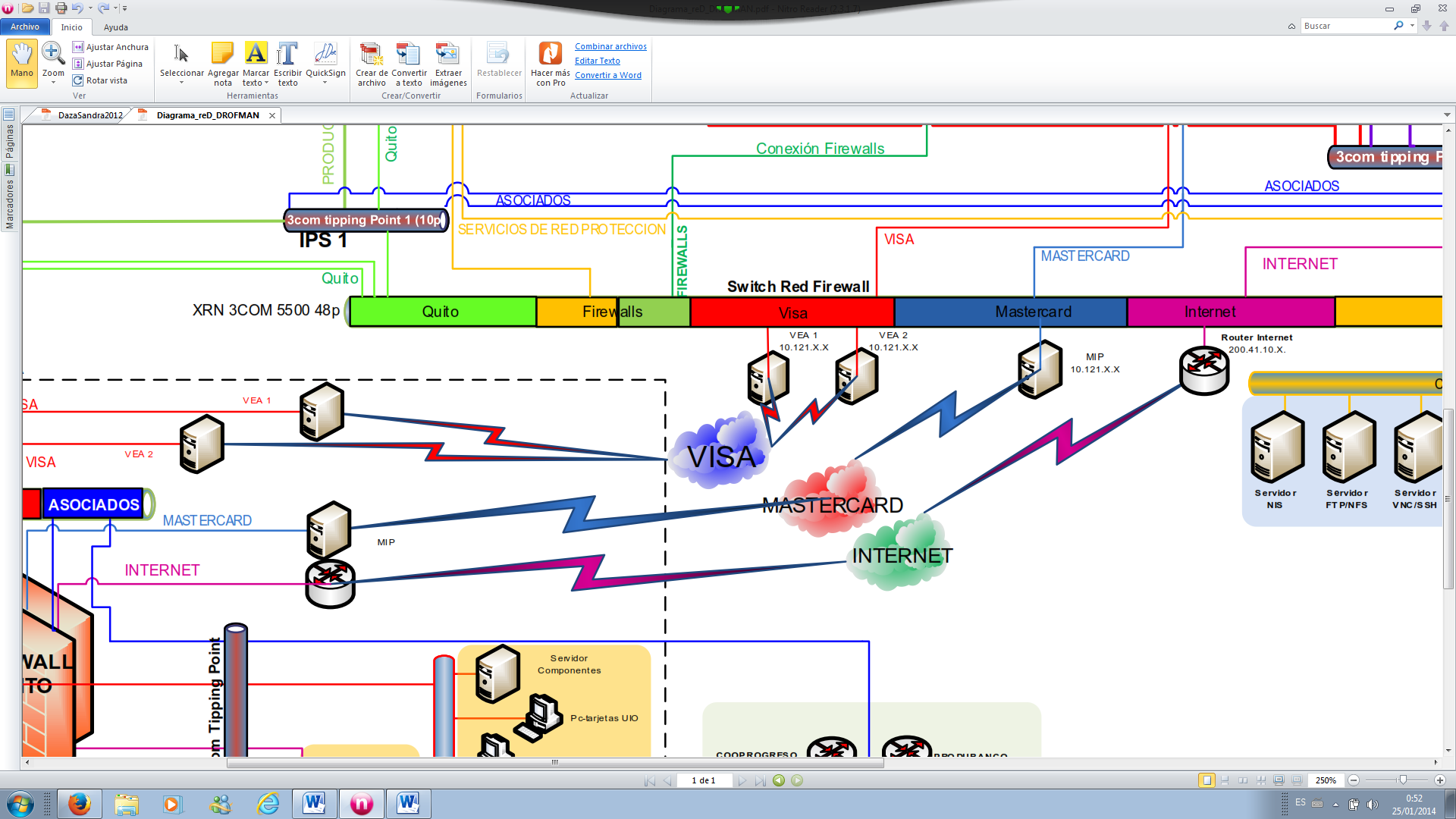
**ANÁLISIS DE LA INFRAESTRUCTURA TI**

**Infraestructura tecnológica de TI.**

**Data Center**

DROFMAN en su sede principal en Guayaquil está conformado de la siguiente manera:

* Tiene equipos de las franquicias (con las debidas certificaciones) de Visa (VEA1 y VEA2), MasterCard (MIP).
* Enlace proporcionado por GLOBAL CROSSING y CLARO en router CISCO más un enlace directo con telefónica a internet con lo cual se establece conexión a la contingencia en Quito.

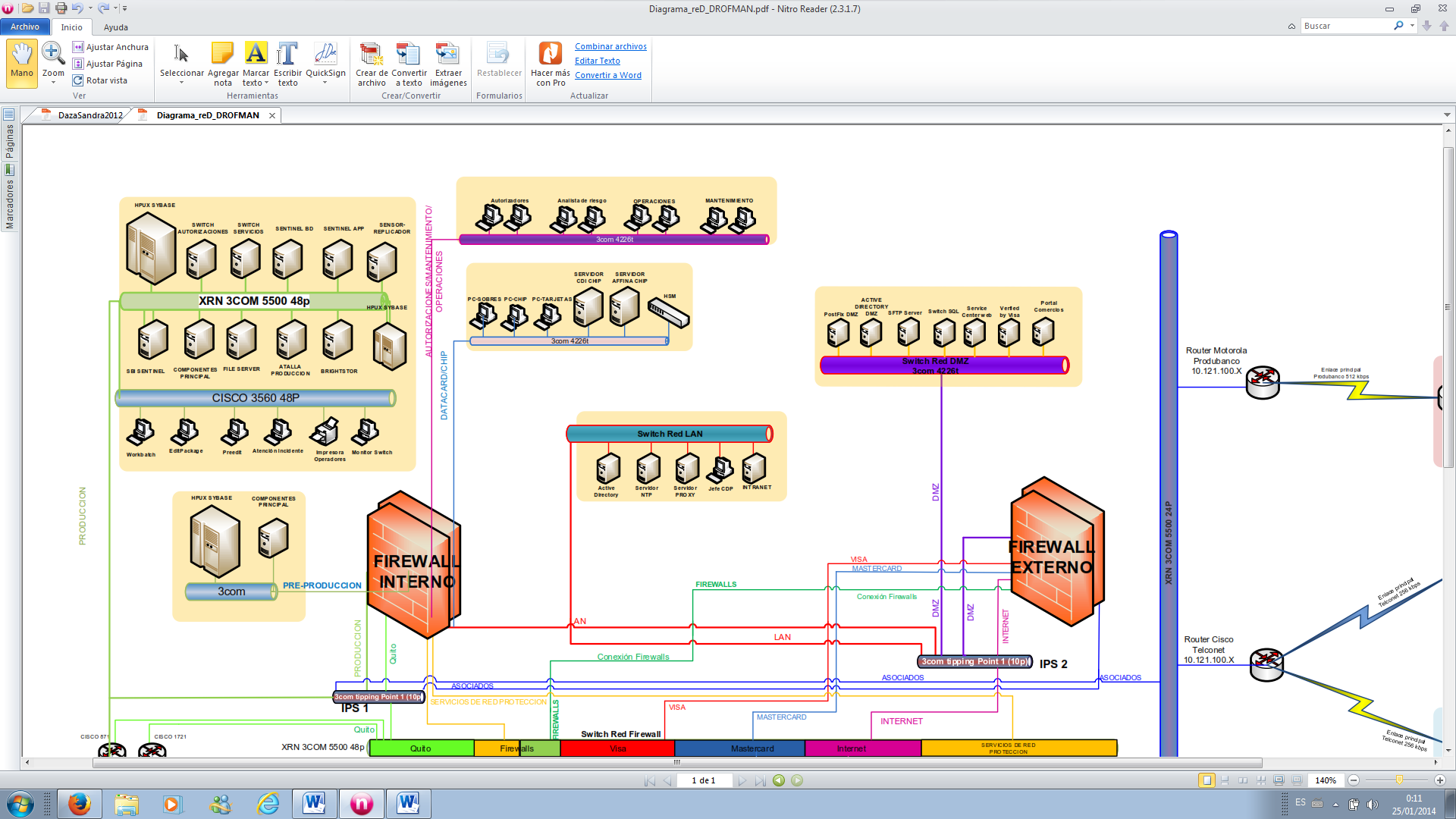


Distribución de Red:

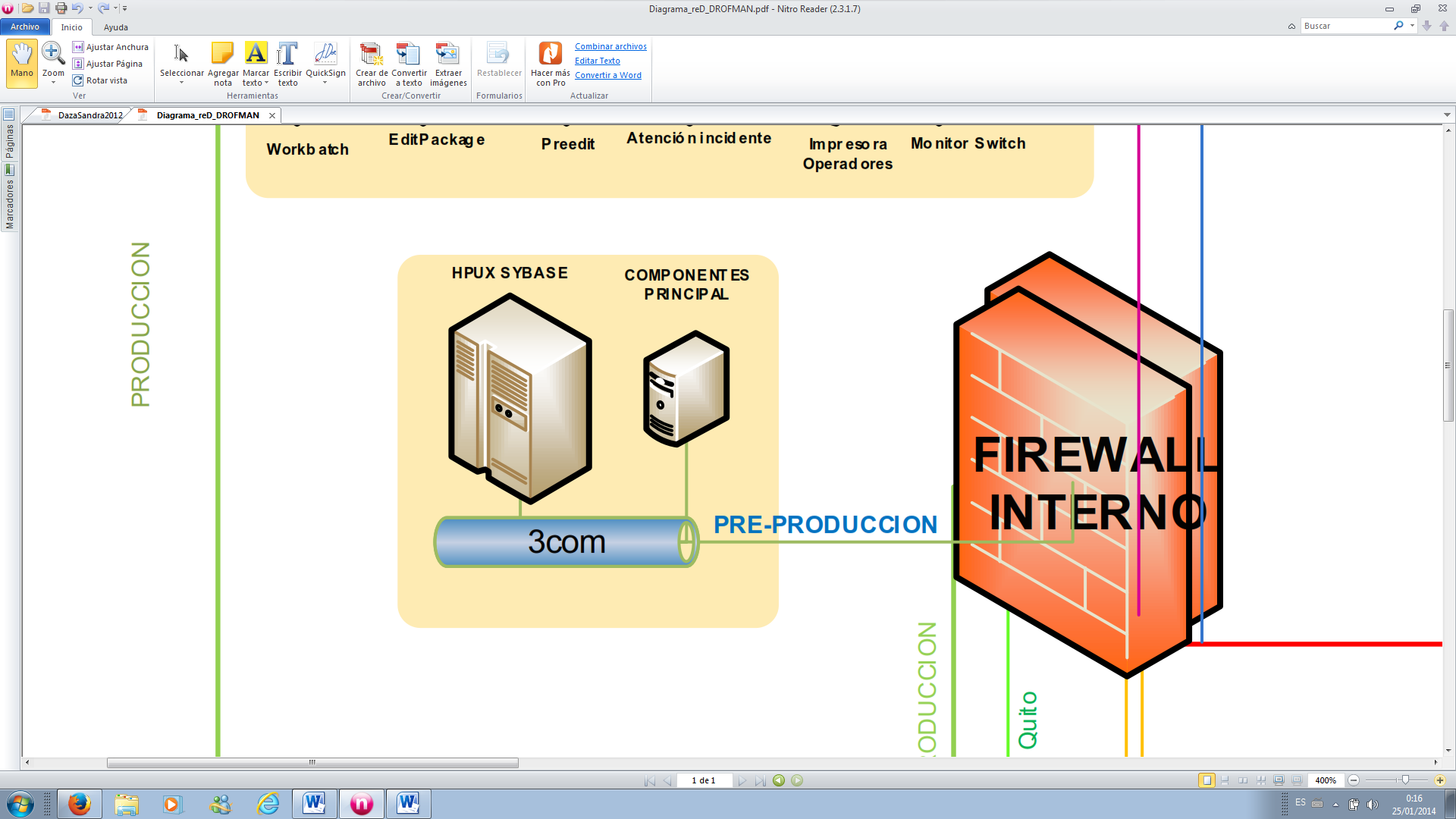
* Red de Producción.
* Red de Pre-Producción.
* Red de Protección.
* Red DMZ.
* Red Datacard/Chip.
* Red LAN.

**Producción.-** comprende un Switch 3COM 5500 al cual se conectan equipos HPUX que comprenden los servidores de: Bases de datos de los Switch Autorizaciones y Servicios, Bases de datos del servidor de Sentinel (moniteoreo de fraudes), Servidor de componentes principales, File Server, Bases de Datos, Brightor (respaldos de bases de datos en tape), Atalla de Producción (manejo de llaves encriptadas para tarjetas de créditos), Replicador de sentinel, Active Directory, Servidores SQUID (Proxy) y Servidor NTP.

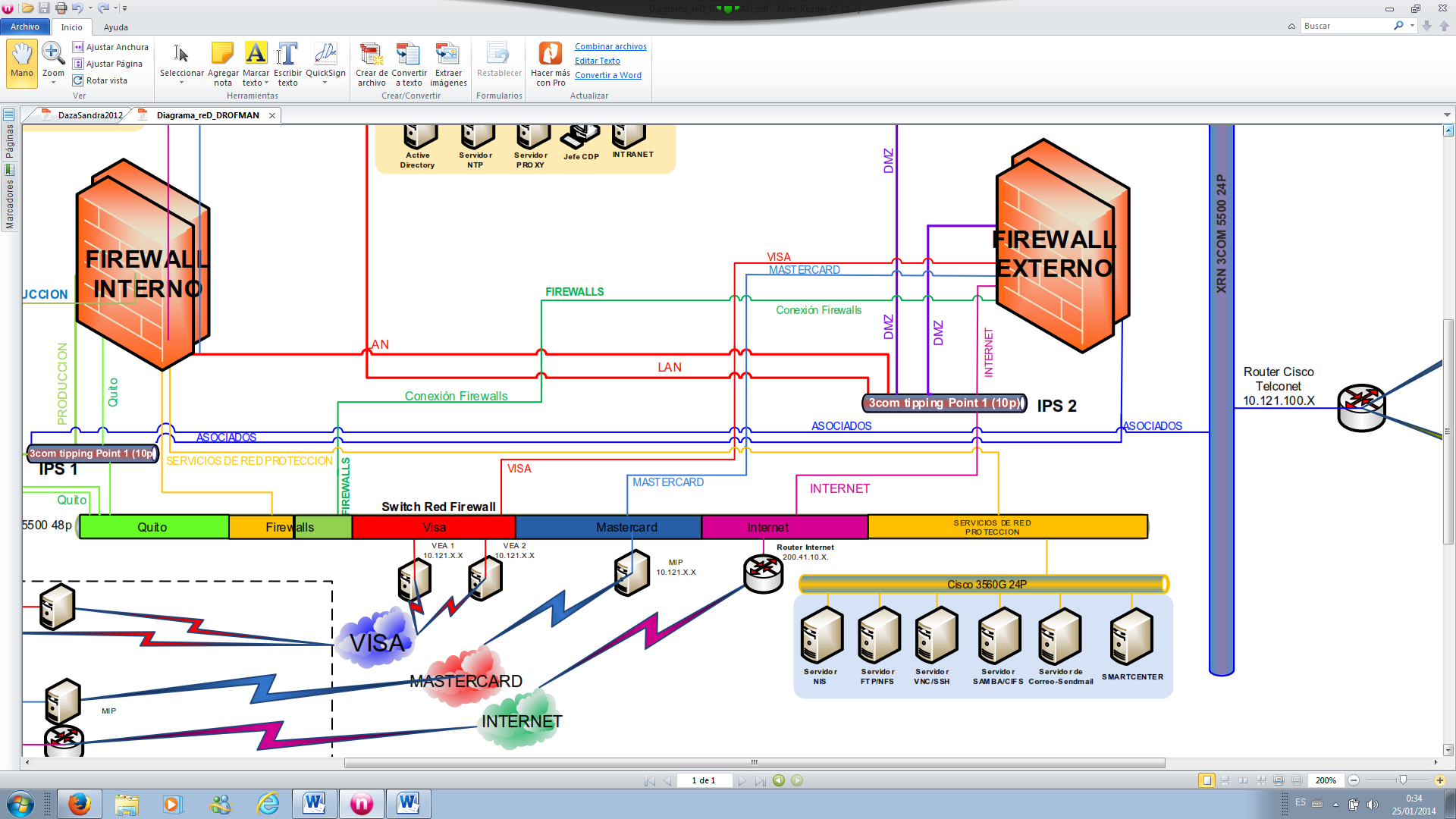
Además se tiene un CISCO 3560 48P en el cual se encuentran las PCs que son utilizadas en el Dpto. del Centro de Cómputo las cuales son utilizadas para monitorear servicios, ejecución de procesos y demás actividades del área.



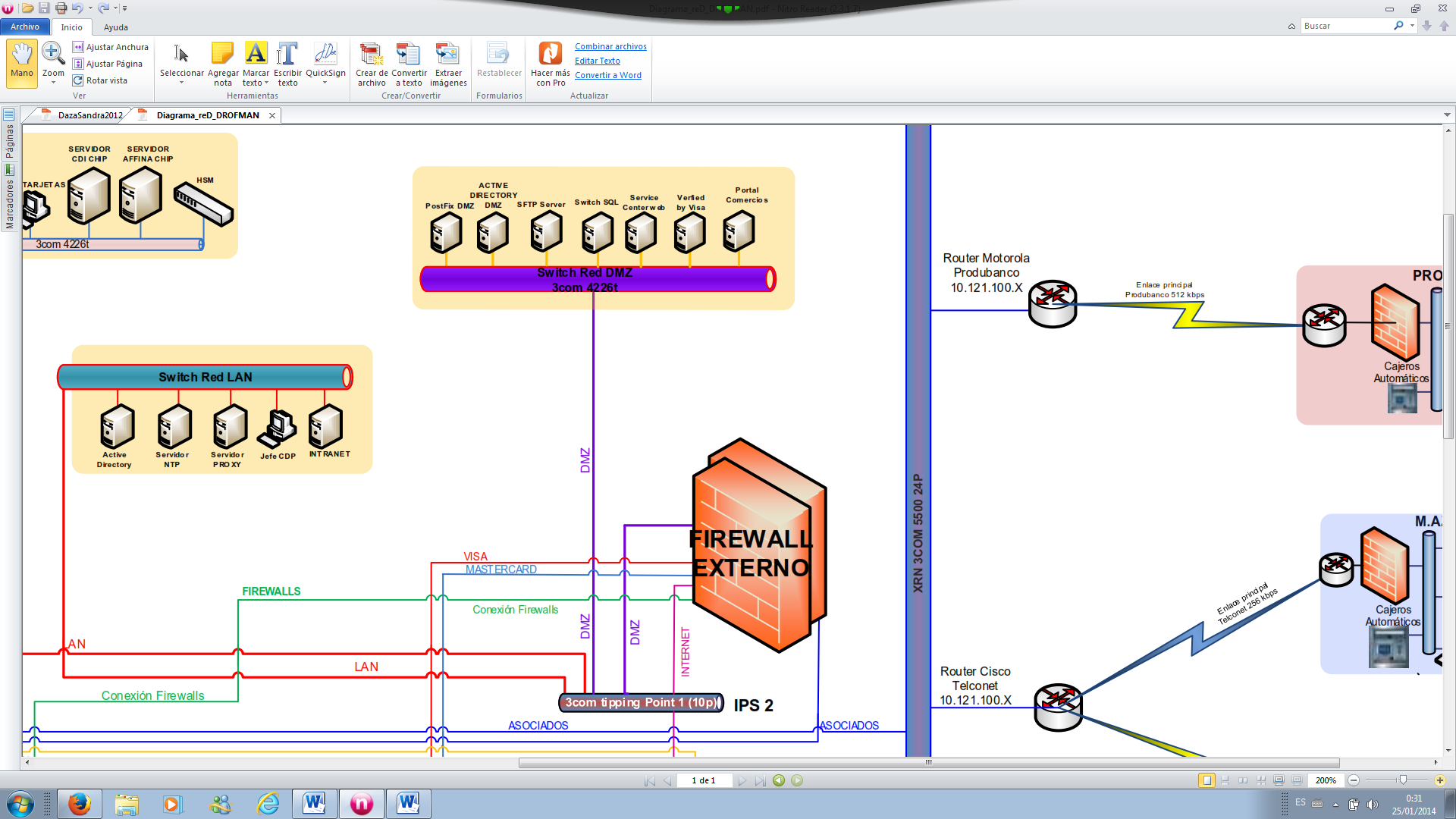
**Preproducción**.- consta de un 3COM a la cual se conecta un Servidor de componentes principal y un Servidor HPUX Sybase direccionadas a un Firewall interno.



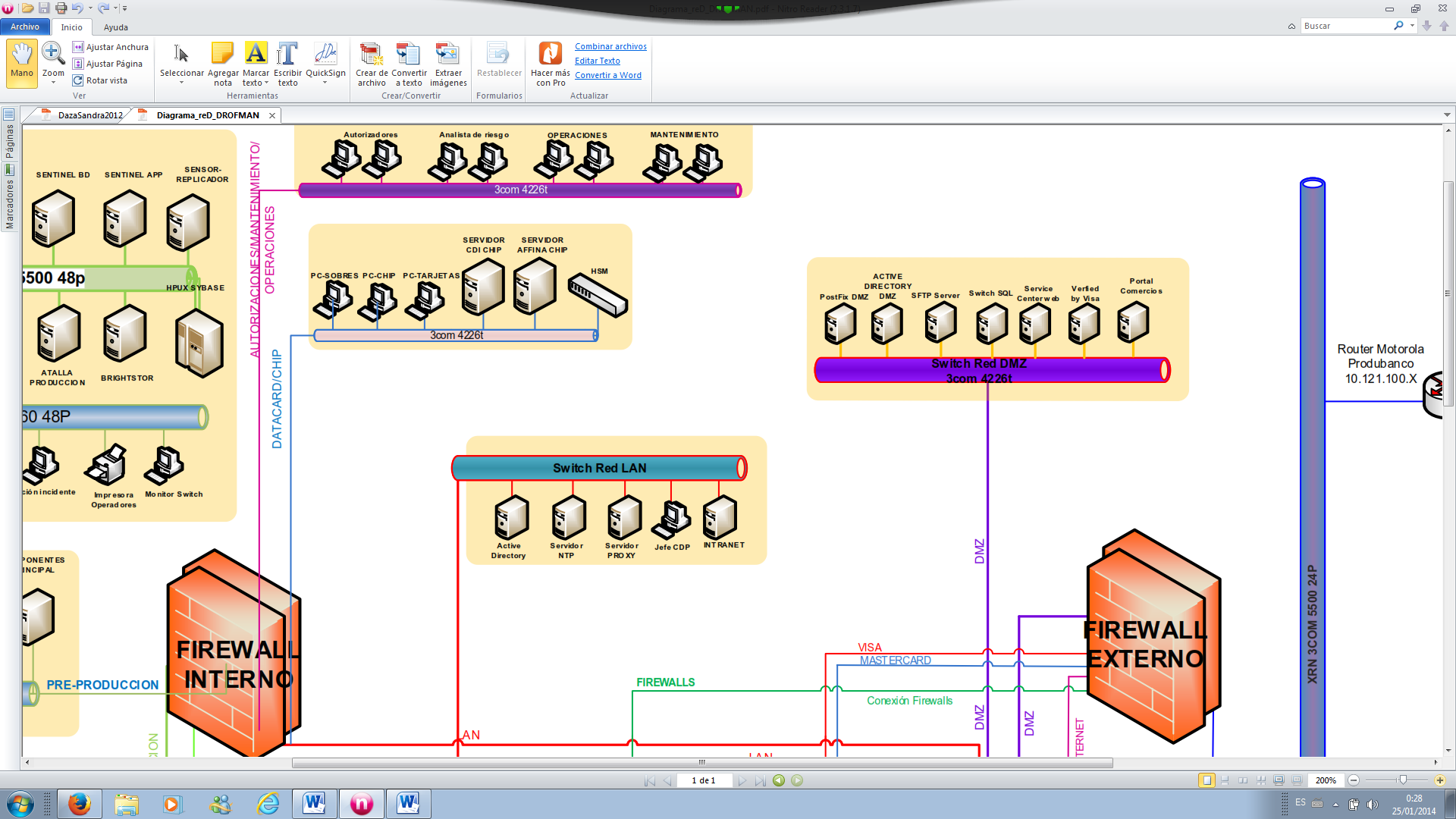
**Protección**.- comprende un CISCO 3560G 24P a la cual se conectan un Servidor NIS, Servidor FTP/NFS, Servidor VNC, Servidor SAMBA, Servidor SSH, Servidor de Correo electrónico y Smart Center.



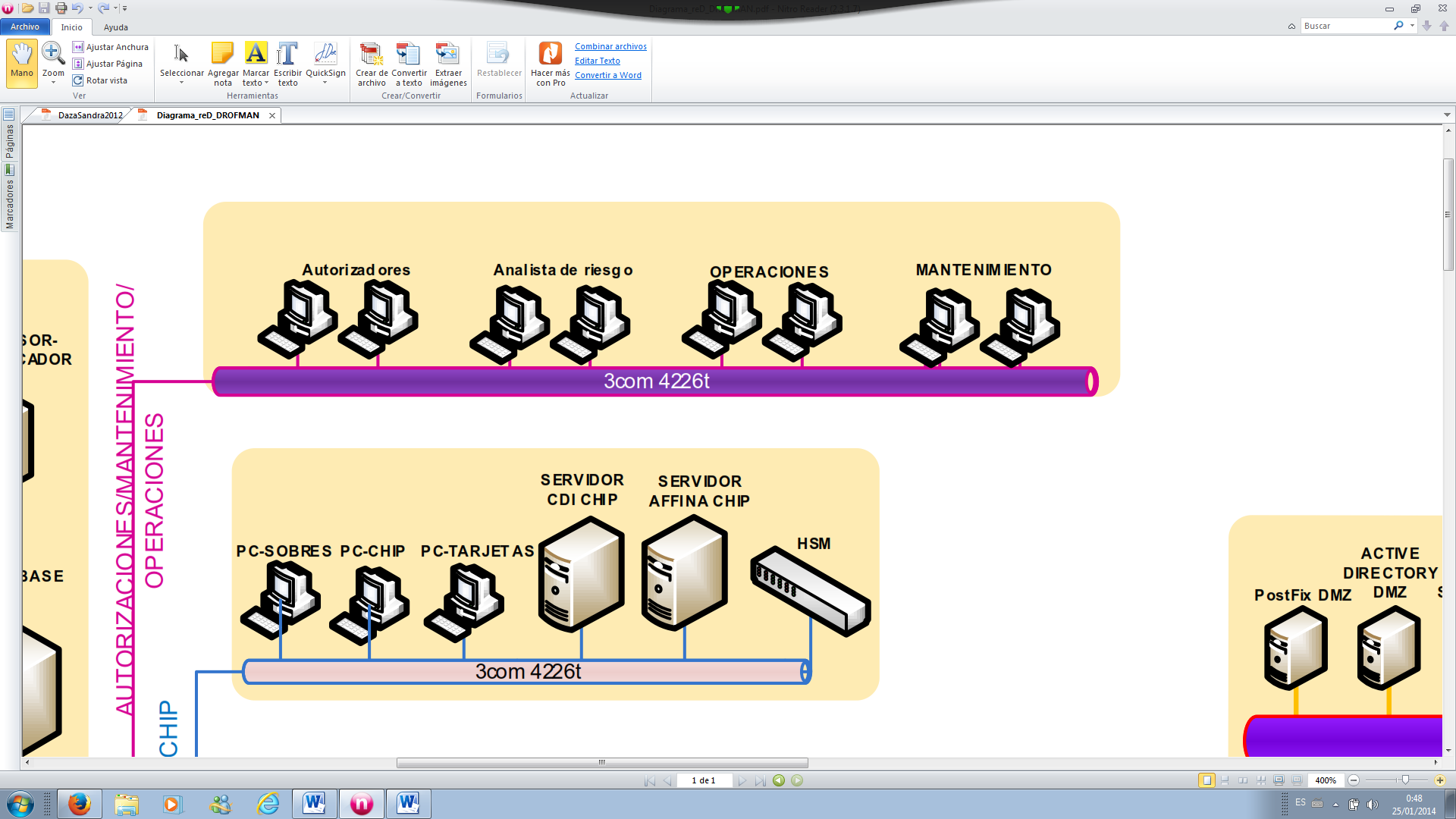
**DMZ.-** se conecta a un 3COM TIPPING POINT 1(10p) pasando por el firewall externo siendo los enlaces principales con las entidades a quienes se brinda el servicio y comprende un Switch 3 COM 4226t a la cual se conectan el Switch de Alignet, Portal transaccional, Active Directory DMZ, SFTP Server (por el cual se envían y reciben archivos de los establecimientos), Service Desk (mesa de ayuda con los bancos) y el servidor de electrónico.



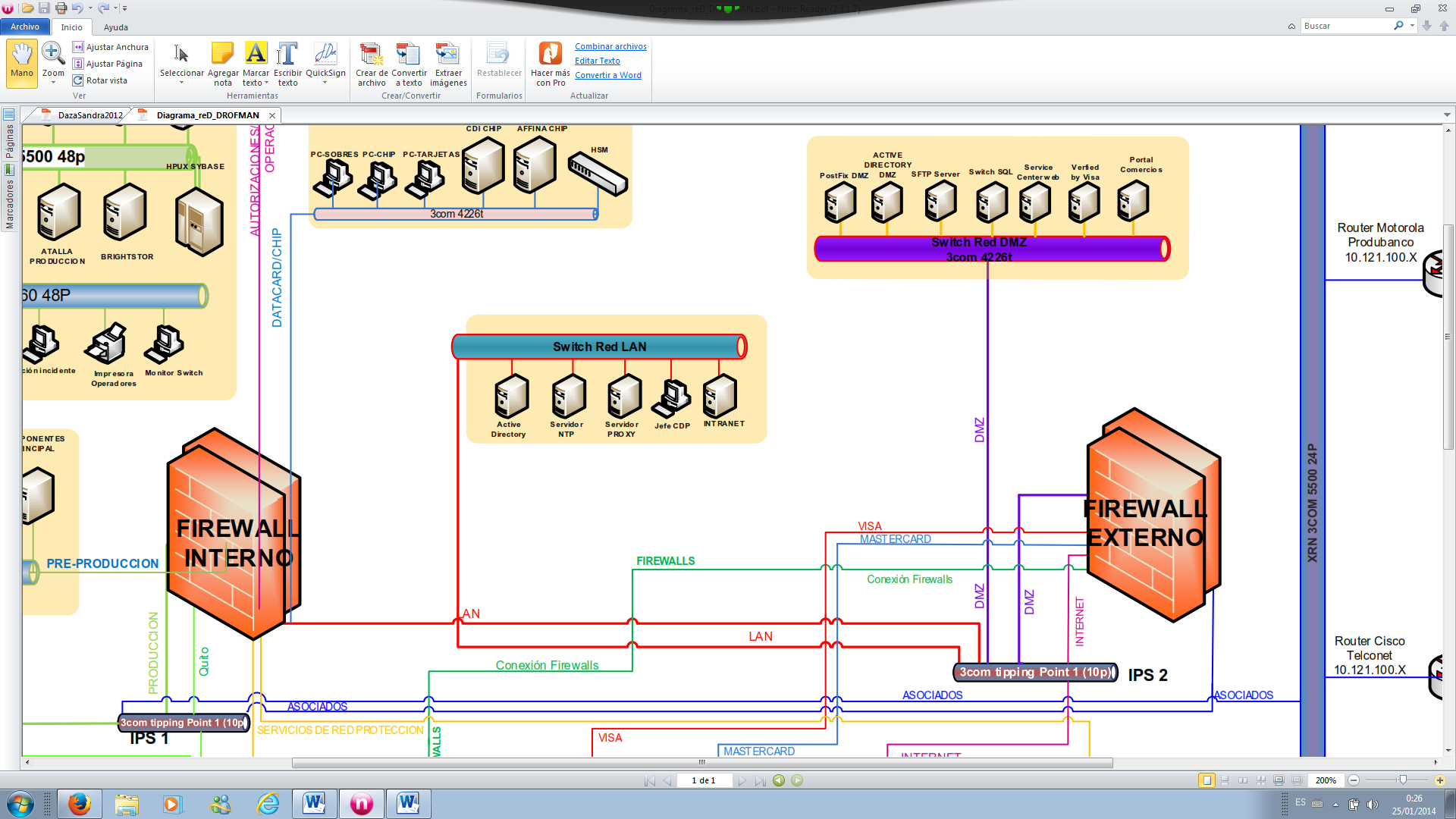
**Datacard/Chip.-** comprende un Switch 3COM 4226t que incluyen Servidores de Chip tanto para impresión de banda como impresión de tarjetas con chip inteligente, adicional sus PCs de personalización y zonificación.



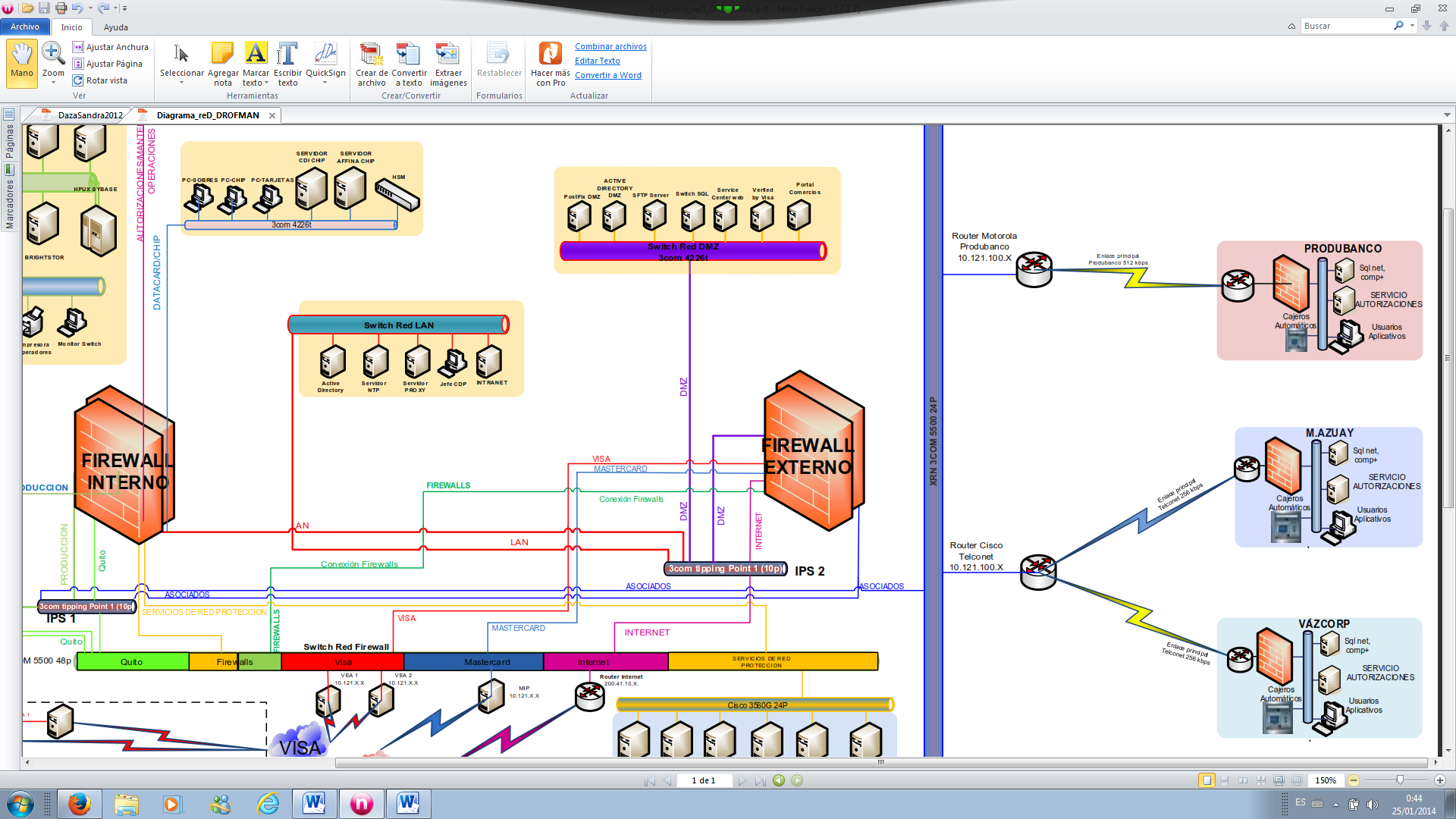
Posee además un Switch 4226t que incluye las PCs de Mantenimiento&Producción, Operaciones, Analistas de riesgo y Autorizaciones manuales.



**LAN.-**  comprende servidores de Active Directory, Servidor NTP, Servidor Proxy y el Servidor de la Intranet.



La conexión hacia los bancos asociados se realiza por un Firewall externo direccionado a un XRN 3COM 5500 24P los cuales van a los ROUTERS (Router Motorola Produbanco y Router CISCO Telconet) los que van a los enlaces principales de cada establecimiento pasando por sus Router y Firewall respectivos.



En su contingencia en Quito está constituida de la siguiente manera:

Tenemos 4 routers distribuidos en 2 lan, 1 DMZ y 1 de Protección de datos PCI.

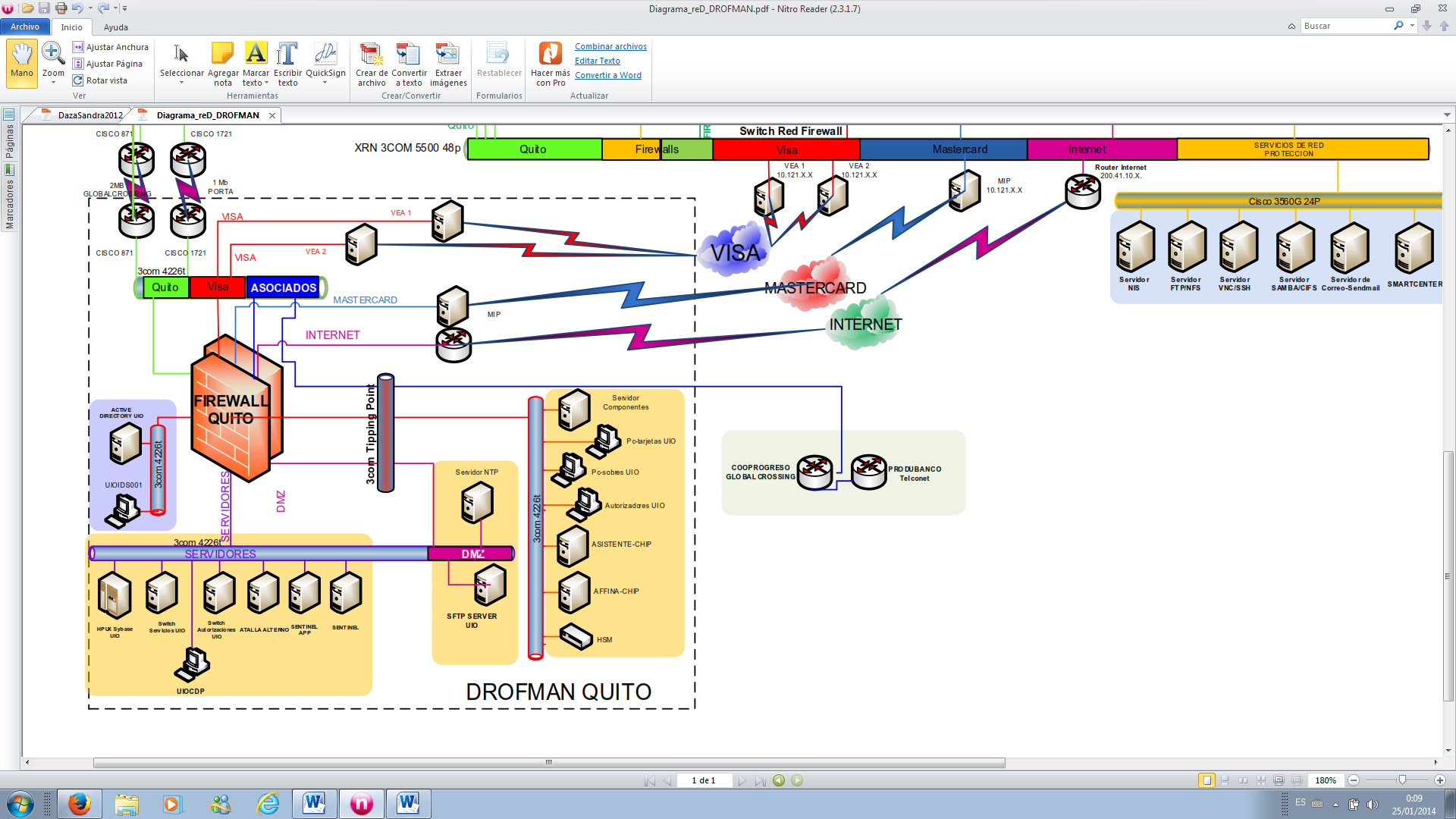
**Lan.-** comprende el Servidor Active Directory, equipos de Sentinel (monitoreo de fraude), Switch de Autorizadores y Servicios, una Base de Datos HPUX Sybase, Atalla Alterno y 2 PCs para procesos y monitoreo en el centro de cómputo.

**DMZ.-** comprende Servidores NTP y SFTP conectados a establecimientos.

**Protección.-** comprende el Servidor de componentes, Chip, HSM, PCs de personalización y zonificación (tarjetas de crédito).

Todo tipo de información transmitida a Quito pasa por el Firewall respectivo el cual permite el paso de la misma a los establecimientos o franquicias respectivamente.

De la misma manera que Guayaquil, el sitio alterno en Quito posee equipos de las franquicias de Visa (VEA1 y VEA2) y MasterCard (MIP) las cuales entran a operar en cuanto se haga el cambio o direccionamiento respectivo y así poder trabajar Quito como centro principal de transmisión y proceso de información a franquicias y establecimientos.



**Lan**

**Wan**

**Seguridades**

**CAPITULO 3:**

**IDENTIFICACIÓN DE VULNERABILIDADES**

**Identificación de Vulnerabilidades**

**Red interna y perimetral.**

**Clasificación de Vulnerabilidades**

**Matriz de impacto en las vulnerabilidades en el negocio**

**CAPITULO 4:**

**IMPLEMENTACIÓN DE SOLUCIONES A LAS VULNERABILIDADES IDENTIFICADAS**

**Aplicación de soluciones en servidores de prueba.**

**Análisis de resultados de impactos en servidores de prueba.**

**Implementación de soluciones según el análisis de resultados de impacto.**

**Implementación de las soluciones en PRE-Producción.**

**Implementación de las soluciones en Producción.**

**Implementación de un plan de prevención contra vulnerabilidades**