**Seguridad De Redes**

**TRABAJO PRÁCTICO**

**Integrantes**: Sebastián Perna

Fabian Moriano

Federico Cristófaro

Facundo Gutierrez

Franco Bertorello

**Cuatrimestre / Año:** 2do 2019

**Docentes:**  Leonardo Gabriele

Ignacio Zugasti

**Índice**

[1. Descripción de la Organización 3](#_Toc25484234)

[2. Diagrama de la Red Actual 4](#_Toc25484235)

[3. Relevamiento de Activos 4](#_Toc25484236)

[4. Análisis de Vulnerabilidades y Riesgos 7](#_Toc25484237)

[5. Políticas de Seguridad: 11](#_Toc25484238)

[6. Soluciones Específicas 13](#_Toc25484239)

[a. A.A.A 13](#_Toc25484240)

[Situación Actual: 13](#_Toc25484241)

[Solución Propuesta 13](#_Toc25484242)

[Especificaciones Técnicas 13](#_Toc25484243)

[b. Firma Digital 13](#_Toc25484244)

[Situación Actual 13](#_Toc25484245)

[Solución Propuesta: 14](#_Toc25484246)

[Especificaciones Técnicas 14](#_Toc25484247)

[c. Seguridad Perimetral 15](#_Toc25484248)

[Situación Actual 15](#_Toc25484249)

[Solución Propuesta / Especificaciones Técnicas 15](#_Toc25484250)

[d. VPN 15](#_Toc25484251)

[Situación Actual 15](#_Toc25484252)

[Solución Propuesta 15](#_Toc25484253)

[Especificaciones Técnicas 15](#_Toc25484254)

[7. Conclusiones 16](#_Toc25484255)

[8. Diagrama de la Red Futuro 16](#_Toc25484256)

[9. Bibliografía 17](#_Toc25484257)

# Descripción de la Organización

Nombre de la empresa: **Full Innovation People** (FIP)

FIP es una empresa fundada en 2004 por Carlos Buenanueva y Roberto Pedraza. Es una agencia de marketing digital dedicada a brindar soluciones de comunicación, vinculadas con plataformas de comunicación online. Sus servicios están destinados a todo tipo de empresas o personajes públicos.

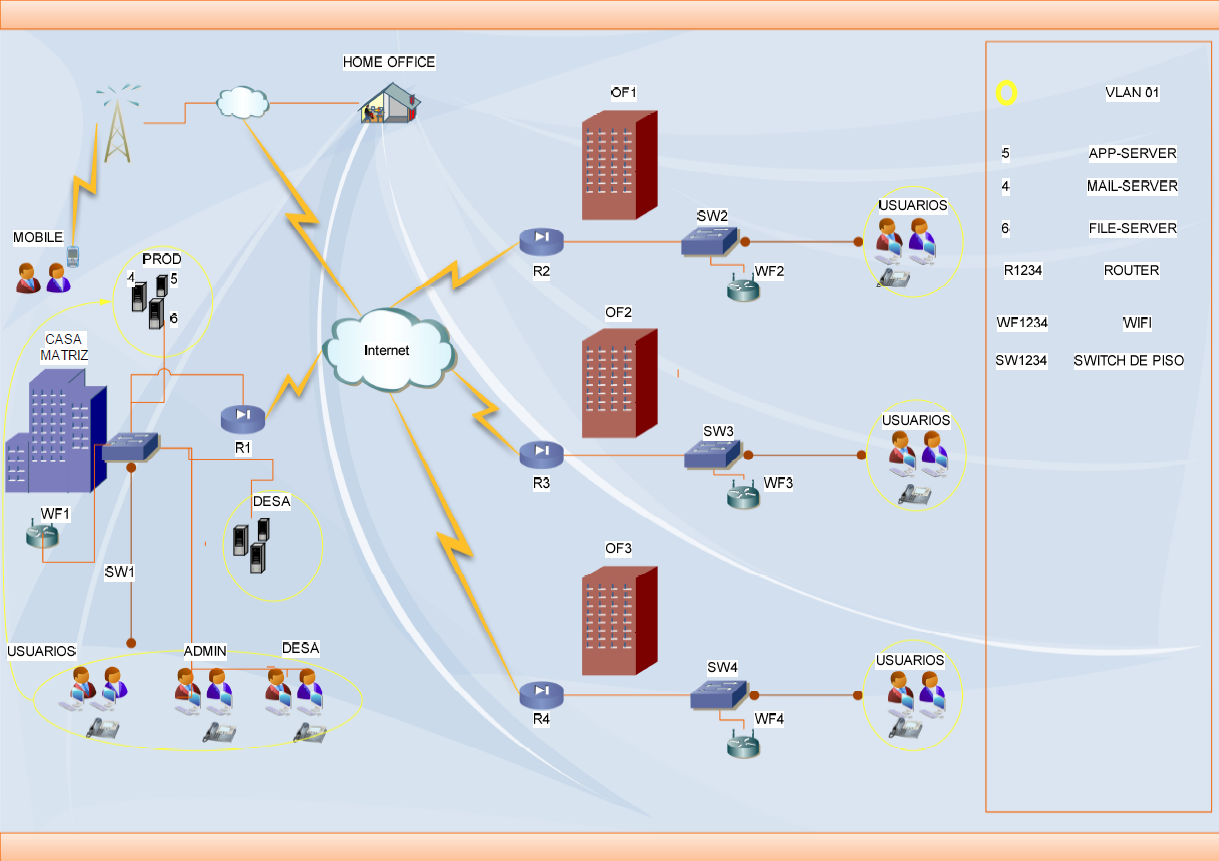
Su misión es la de satisfacer a sus clientes, brindando soluciones y servicios de marketing digital con foco en la innovación y que permitan impulsar su potencial como empresa.

Actualmente cuenta con 84 empleados distribuidos en sus 4 sedes, 2 en Capital, 1 en ciudad de Córdoba y otra en ciudad de Mendoza. La sede principal es la oficina administrativa ubicada en la Ciudad de Buenos Aires, en Avenida Brasil 1022. Sus 3 oficinas anexas ubicadas en el barrio de Belgrano de la Ciudad de Buenos Aires, otra en el Barrio Gral. Paz de la ciudad de Córdoba y la más nueva en el centro de la ciudad de Mendoza. Las 3 sirven de oficina para los empleados especialistas en marketing y comerciales.

En la comercialización de sus distintos servicios, FIP diseña planes de marketing digitales, administran redes sociales, crean contenido digital, entre otros servicios. Basa su esquema de rentabilidad en el servicio mensual que ofrece a las empresas y personas individuales que contratan el servicio.

FIP ofrece un sitio web y una aplicación mobile que permite a sus clientes administrar algunos de sus servicios. A través del sitio o la aplicación mobile los clientes pueden cargar pedidos, intercambiar información confidencial para cada trabajo, intercambiar archivos multimedia, aprobar prototipos, entre otras cosas.

# Diagrama de la Red Actual



# Relevamiento de Activos

|  |  |  |
| --- | --- | --- |
| Activo | Descripción | Cantidad |
| Hardware | | |
| Servidor de mail | Servidor que presta el servicio de correo electrónico | 1 |
| Servidor aplicativo | Servidor que presta el servicio aplicativo | 1 |
| Servidor de archivos | Servidor que presta el servicio de guardado de archivos | 1 |
| Servidor de desarrollo | Servidor de ambiente de pruebas | 3 |
| Estación de trabajo de escritorio y/o portátil | Equipamiento de escritorio (PC o notebook) | 93 |
| Teléfono de línea | Equipamiento de comunicación telefónica | 93 |
| Router | Dispositivo de red de enrutamiento | 4 |
| Router Wifi | Dispositivo de red de servicio de conexión inalámbrica | 4 |
| Switch | Dispositivo de red de interconexión de equipos | 4 |
| Impresora | Dispositivo para impresión de documentos | 7 |
| Modem | Dispositivo para la conexión a internet | 4 |
| Software | | |
| Sitio Web Externo | Página web de acceso interno y externo | 1 |
| Aplicación Móvil Externa | Aplicación de celulares de acceso externo | 1 |
| Base de datos empleados | Base de datos con información de empleados de la empresa | 1 |
| Base de datos clientes | Base de datos con información de clientes | 1 |
| Personal | | |
| Personal administrativo | Personas correspondientes a presidencia, gerencia, comerciales, contaduría, legales, administración y recepción | 28 |
| Personal de sistemas | Personas correspondientes a áreas de tecnología, seguridad, desarrollo y soporte técnico | 8 |
| Personal de seguridad física | Personas correspondientes a tareas de seguridad en las oficinas | 4 |
| Personal de marketing digital | Personas correspondientes a tareas de marketing digital | 44 |
| Infraestructura Edilicia | | |
| Edificio | Oficinas físicas | 4 |
| Datacenter | Centro de Operaciones de Datos | 1 |
| Cuarto de racks | Espacio físico designado al equipamiento de conexión de redes | 4 |

# Análisis de Vulnerabilidades y Riesgos

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID Amenaza | Activo | Vulnerabilidad | Amenaza | Riesgo o Impacto | Probabilidad | ID Politica |
| 1 | Servidores (todos) | Sistemas operativos no cuentan con las últimas actualizaciones de seguridad. | Posible infección de malware por atacante externo a la empresa. | Alto | Alta | 1 |
| 2 | Servidor de mail | Archivos adjuntos no son analizados por un antivirus tras la llegada al servidor de mail. | Posible infección de malware por atacante externo a la empresa. | Alto | Alta | 2 |
| 3 | Router (todos) | Firmware de equipamiento desactualizado. | Posible ingreso a la red por atacante externo a la empresa | Alto | Media | 7 |
| **4** | Red General | Conexión de red entre oficinas con servicios de terceros sin garantía de privacidad y con vulnerabilidades de seguridad. | Posible robo o hurto de información por atacante externo o ingreso de personas no autorizadas | Alto | Media | 16 |
| **5** | Bases de datos de empleados | Motor de base de datos no cuenta con las últimas actualizaciones disponibles. | Posible ataque externo mediante explotación de vulnearabilidad puede obtener datos confidenciales y/o denegar servicios | Medio | Baja | 1 |
| **6** | Estaciones de trabajo | Acceso a sistema operativo mediante usuarios locales sin control ni gestión centralizada. | Posible ingreso de empleados no autorizados que pueden robar datos confidenciales y/o impersonarse con un usuario no asignado. | Medio | Media | 3, 7 |
| **7** | Acceso a sistema operativo con privilegios sin control ni gestión centralizada. | Posible robo de información, instalación de software no licenciado o inseguro y/o infección de malware por empleados. | Alto | Alta | 4 |
| 8 | Equipamiento portátil sin candados físicos. | Posible hurto de hardware por personal de limpieza. | Medio | Baja | 5 |
| 9 | Equipamiento portátil sin discos cifrados | Posible hurto de información por robo de equipamiento en la vía pública. | Medio | Media | 6 |
| 10 | Antivirus desactualizados. | Posible infección de malware por atacante externo a la empresa. | Alto | Alta | 7 |
| 11 | Sistemas operativos no cuentan con las últimas actualizaciones de seguridad. | Posible infección de malware por atacante externo a la empresa. | Alto | Alta | 8 |
| 12 | Acceso remoto mediante TeamViewer Free | Posible ataque de Man-in-the-middle por atacante externo. | Medio | Media | 9 |
| **13** | Acceso a internet sin restricciones ni control. | Posible infección de malware por empleados que accedan a sitios inseguros con posibilidad que estos descarguen malware. | Alto | Alta | 10 |
| 14 | Impresora | Impresión sin control de acceso. | Posible robo de documentos con información sensible por empleados. | Bajo | Baja | 11 |
| 15 | Oficinas | Acceso a la oficina física sin control de seguridad. | Posible ingreso de personas no autorizadas que pueden dañar o robar el equipamiento, implantar equipos no autorizados y/o robar información confidencial. | Alto | Media | 12 |
| 16 | Acceso a cuarto de racks sin control de seguridad. | Posible ingreso de personas no autorizadas que pueden dañar o robar el equipamiento o implantar equipos no autorizados. | Alto | Media | 13 |
| 17 | Personal (todos) | Personal sin capacitación sobre temas importantes de seguridad. | Posible infección de malware por atacante externo a la empresa. | Medio | Alta | 5, 14 |
| 18 | No existe un acuerdo de confidencialidad firmado por los empleados. | Posible robo de información sensible por parte de los empleados. | Bajo | Baja | 15 |
| 19 | Información | Documentación electrónica fácilmente alterable. | Posible modificación por suplantación de identidad. | Alto | Alta | 6, 17 |
| 20 | No existe una solución para prevenir la fuga de información. | Posible robo de información sensible por parte de los empleados. | Alto | Alta | 6, 18 |

# Políticas de Seguridad:

El presente documento es aplicable a todos los empleados, sean internos o externos a la organización, incluyendo a todo el personal que en algún momento cuente con acceso a los recursos, sean o no informáticos, y/o información de la empresa. Se detallan a continuación las políticas aplicadas:

|  |  |  |
| --- | --- | --- |
| ID Política | Descripción Política | ID Amenaza |
| 1 | Establecer un procedimiento de implementación y verificación regular de Fixes de seguridad sobre todos los servidores de la empresa, garantizando ejecutar la correcta actualización dentro de la primer semana luego de la publicación del fix. | 1, 5 |
| 2 | Establecer un firewall previo a la llegada de archivos al servidor de correo electrónico. Implementar un IDS para analizar anormalidades en el tráfico de la red. | 2 |
| 3 | Implementar un servicio de Active Directory para la administración de privilegios en perfiles y grupos de usuarios, estableciendo un acceso seguro a los recursos claves de la empresa | 6 |
| 4 | Implementar grupos de Administradores Locales, en los cuales se agregarán solo aquellos usuarios de sistemas que requieran dicho perfil. | 7 |
| 5 | Diseñar canales de comunicación corporativa, adjuntando un documento electrónico donde se detallen todas las recomendaciones aplicadas al uso de los equipos móviles, como las responsabilidades inherentes al activo TI, que tendrá el usuario final al recibir el mismo. | 8,17 |
| 6 | Implementar un software de cifrado de disco rígido, garantizando la absoluta seguridad de la información almacenada en el medio. | 9 |
| 7 | Establecer planes de obsolescencia de software cross a la organización, describiendo planes de actualización continua de aplicaciones, sistemas operativos firmware y hardware, asegurando contar con los últimos builds instalados en todos los dispositivos. Deben existir planes de actualización para agentes del antivirus corporativo, como flujos de soporte inmediato para aquellas alarmas sobre equipos que tengan presenten algún incidente con el antivirus. | 3, 6 |
| 8 | Deben existir procedimientos de implementación y verificación regular de Fixes de seguridad de sistema operativo sobre todas las PCs y Notebooks de la empresa. | 11 |
| 9 | Instalar la funcionalidad de VPN IPSec para garantizar la seguridad de la comncaciion y disminuir el riesgo de un ataque. | 12 |
| 10 | Definir diferentes niveles de acceso a internet, estableciendo dichos niveles por grupos/sectores y globales a la organización. | 13 |
| 11 | Definir un método de autenticación físico con tarjeta corporativa, a través del cual se ejecute una validación previa a que el usuario retire las impresiones ejecutadas. | 14 |
| 12 | Definir un método de autenticación físico con tarjeta corporativa para acceder a las oficinas de la organización. | 15 |
| 13 | Definir un método físico de autenticación mediante una tarjeta corporativa y un workflow de autorización, a través del cual se ejecutará un proceso de aprobaciones. | 16 |
| 14 | Establecer cursos interactivos con material multimedial y publicarlos en la intranet corporativa. Concientizar al personal de la obligatoriedad de cumplimiento de dichos cursos. | 17 |
| 15 | Implementar un acuerdo de confidencialidad digital, para todo nuevo ingresante, y establecer un circuito de revisión del mismo para todo empleado de la organización. El mismo debe ser revisado y vuelto a firmar cada 2 años. | 18 |
| 16 | Implementar un mecanismo de conexión segura entre oficinas, que permita asegurar el flujo de paquetes, garantice la autenticación mutua y brinde seguridad en la conexión. | 4 |
| 17 | Implementar un sistema de firma digital que pueda atribuir el documento a su autor (una persona) en forma fehaciente (autenticar al autor), verificar la no alteración del contenido del documento luego de ser firmado (integridad del contenido) y garantizar el no repudio. | 19 |
| 18 | Implementar un sistema mediante políticas de DLP y control granular de dispositivos para restringir el uso de unidades USB, dispositivos móviles conectados a USB, grabadoras de CD/DVD, almacenamiento en la nube y otros medios extraíbles. | 20 |

# Soluciones Específicas

# A.A.A

### Situación Actual:

La empresa no cuenta actualmente con un proceso de autenticación y autorización de los usuarios ni de auditoria, donde no registra la gestión de los usuarios que acceden a la red ni controla los recursos utilizados. Tampoco cuenta con la red WiFi protegida.

### Solución Propuesta

Se recomienda actualizar y configurar la arquitectura que contempla la autenticación, autorización, contabilización y auditoría de información confidencial.

Para ello, se propone implementar los siguientes protocolos.

### Especificaciones Técnicas

* **Implementación del protocolo LDAP a través del servicio Active Directory (AD):** Los usuarios de la red estarán registrados en un directorio (AD) junto a sus permisos, grupo, políticas de acceso y asignación de recursos.
* **Configuración de un RADIUS wireless server:** Será configurado un servidor RADIUS para autenticar los usuarios que deseen ingresar a la red WiFi.
* **Implementación de soluciones de detección de fugas de información y prevención (DLP):** Se implementan dichas soluciones para controlar la fuga de información sensible

por parte de los usuarios.

# Firma Digital

### Situación Actual

Hoy en día, la empresa no cuenta con un sistema de firma digital para sus documentos en general, desde la facturación enviada a sus clientes, como hasta en procesos internos. Por nombrar algunos de ellos, podemos mencionar la emisión de recibos de sueldo a sus empleados.   
  
Toda la información se encuentra en papel resguardada en armarios, existen procesos de escaneo de documentación firmada en forma manuscrita y enviadas por mail. No existe ningún tipo de validación de integridad y no repudio sobre los documentos electrónicos que circulan en la empresa.

### Solución Propuesta:

La implementación de un sistema de Firma Digital. Poder enviar un documento firmado a través de medios electrónicos de manera que ese documento cuente, por lo menos, con las mismas características técnicas de seguridad y legales que tiene un documento firmado a mano.

* **Relevamiento de los procesos candidatos a su implementación:** Se han relevado y analizado todas las metodologías claves de la empresa, detectando los procesos que deben firmarse digitalmente.
  + **Facturación a Clientes:** La firma de estos documentos, al momento de su generación, permitirá garantizar su integridad y asegurar que no fueron modificados, asegurando al receptor que quien lo haya firmado sea quien dice ser.
  + **Emisión de Recibos de Sueldo a Empleados**: El objetivo es garantiza la aceptación y firma del recibo por parte del empleado.

### Especificaciones Técnicas

Utilizar un método de criptografía asimétrica con un par de claves (pública y privada) de modo tal que lo que se cifra con una clave sólo pueda descifrarse con la otra, siempre en forma conjunta. La clave pública se distribuye y la clave privada la conserva el propietario, protegida por una contraseña que sólo él conozca.  
  
El proceso de firma digital se compone de los siguientes puntos:

1. Se genera un hash al documento en particular que ante cualquier alteración creará un hash diferente al generado originalmente.
2. Este hash se encripta con la clave privada del firmante, agregando su clave pública son la combinación que terminan formando la firma digital, la cual se agrega al documento y estará listo para ser distribuido.

**Algoritmos que se utilizaran en ambos procesos (Firma Digital y Firma Electrónica)**

Para la implementación del proceso **Firma Digital**, utilizaremos **RSA** como algoritmo de clave publica y **SHA 256** como mecanismo de Hash. Este proceso se aplicará tanto para el envío de facturas a clientes, como también para el proceso de entrega de recibos de sueldo.

Para asegurar que el dueño de la clave publica es quien envío el documento con la firma digital adjunta, implementaremos un proceso de certificados digitales, a través de la Autoridad Certificante de la oficina nacional de tecnologías de información. **Este proceso aplica al envío de Facturas a clientes.**  
  
Cada empleado con firma digital deberá contar con un Dispositivo Token FIPS 140 2 nivel 2 o superior y tener instalados en los equipos los certificados (RAÍZ y AC).

# Seguridad Perimetral

### Situación Actual

La Empresa no cuenta con un dispositivo de seguridad que permita proteger los equipos individuales, servidores o equipos conectados en red contra accesos no deseados de intrusos que pueden robar datos confidenciales, hacer perder información valiosa o incluso denegar servicios en la red.

Tampoco dispone de un sistema de detección de intrusiones ni una seguridad intermedia para alojar los servicios que van a ser expuestos a internet minimizando el impacto de un posible ataque.

### Solución Propuesta / Especificaciones Técnicas

* **Implementar un IDS/IPS Server:** Será configurado un servidor IDS/IPS para la detección de accesos no autorizados y el análisis de tráfico de los puertos del firewall. Para esto se instalará un NIDS con específicas reglas.
* **Implementar una DMZ:** Se implementará una DMZ para los servidores más expuestos a ataques, que son los servidores de mail, sandbox y anti-spam.
* **Configuración de Firewall para toda la red:** Se tendrá configurado un firewall corporativo en la casa matriz y distintos firewalls para las oficinas (SOHO). También se debe considerar que todas las máquinas de la empresa tendrán un firewall personal activo.

# VPN

### Situación Actual

Actualmente la empresa no cuenta con un sistema de conexión entre oficinas y acceso remoto, por lo que utilizan herramientas externas gratuitas como TeamViewer. Dicha solución no es segura y fue implementada como una alternativa por los mismos usuarios. Esta forma de operar no está autorizada ni cumple con los requerimientos de seguridad ni de comunicaciones. Es por eso que se debe tomar una acción de corrección de la situación.

### Solución Propuesta

A raíz de la situación actual se propone implementar una solución de VPN que permita resolver las vulnerabilidades relacionadas a la interconexión de redes distantes y el acceso remoto. La implementación de esta solución busca asegurar la comunicación y garantizar la autenticación, tanto para la conexión entre oficinas como para el acceso remoto de empleados.

### Especificaciones Técnicas

Implementación de una VPN con uso de la suite de protocolos IPSec que provee seguridad a las comunicaciones hacia Internet a nivel de la capa de red (IP). Su implementación aplica en el caso de la interconexión entre oficinas mediante la solución “Site to Site” y para el caso de acceso remoto de empleados mediante la solución “Host to Site”. Esta implementación permitirá garantizar la autenticación, asegurar el flujo de paquetes y brindar confidencialidad.

Para el proceso de uso se deberán configurar usuarios y contraseñas que permitan a los empleados conectarse remotamente a sus puestos de trabajo. El acceso debe ser justificado para todos los casos indicando los días y horario de sesión habilitada. Esta solución permitirá la conexión remota para soporte o bien para realizar home office.

Para la implementación de VPN IPSec se utilizará el modo túnel para la transmisión y los siguientes los protocolos:

* IKE v2, para la negociación de llaves en IPSec.
* AH, protocolo que agrega encabezados de paquetes para el manejo de autenticación.
* ESP, protocolo para la confidencialidad mediante el encapsulamiento seguro del paquete.
* AES, para algoritmo de cifrado.
* SHA1, para algoritmo de autenticación de mensajes hash.

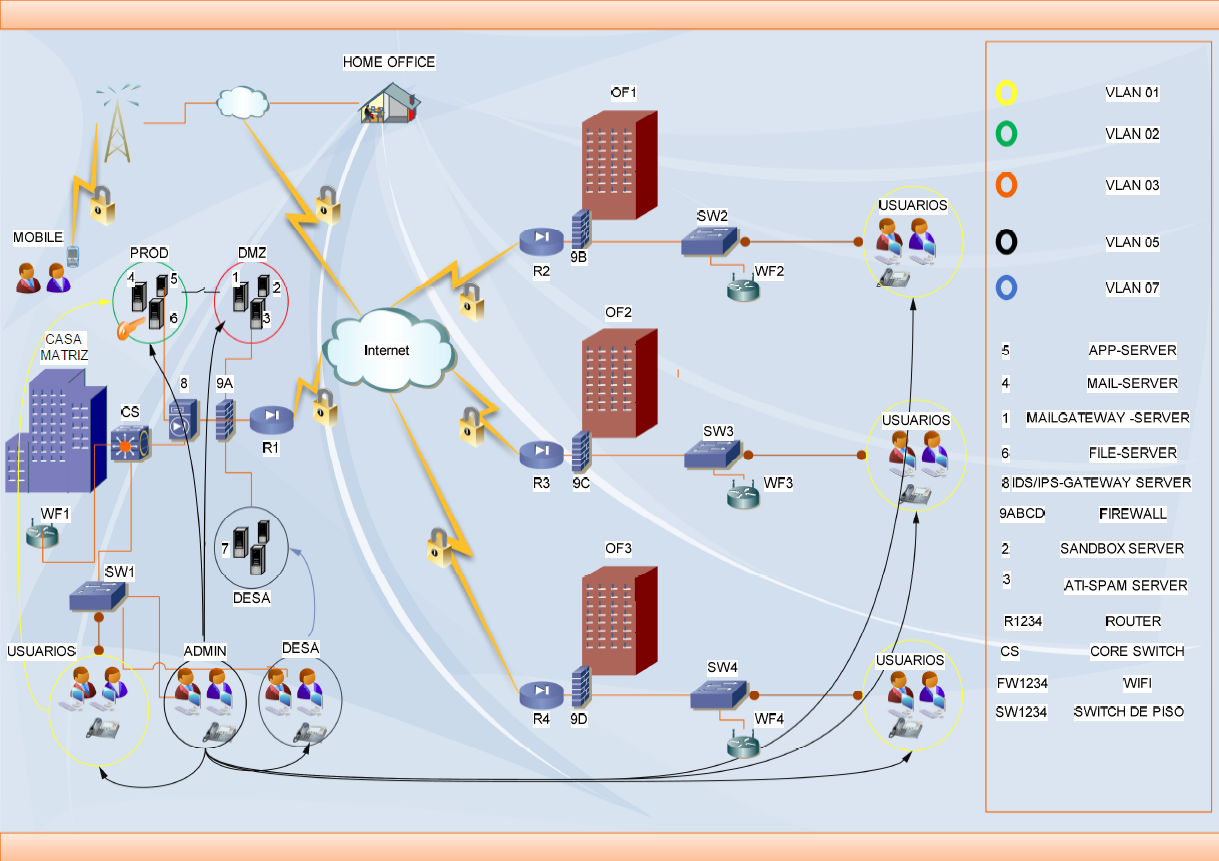
# Conclusiones

En base al análisis realizado, se han implantado políticas de seguridad para minimizar los riesgos que pueden ocasionar pérdidas importantes en la entidad. Adicionalmente se han implementado protocolos de seguridad para asegurar una comunicación entre las partes involucradas con la empresa, y aún los clientes externos, de manera de proteger la información, y el acceso a los datos de quienes no tienen autorización.

Mediante estos recursos, se busca lograr que los sistemas de información y redes de la empresa estén disponibles, y sean accedidos única y exclusivamente por quienes tienen autorización para hacerlo.

Mediante la implementación de todos estos recursos buscamos lograr contar con todos los atributos de la Seguridad en esta Entidad: Integridad, Confidencialidad, Disponibilidad, Autenticación, y No Repudio.

# Diagrama de la Red Futuro



# Bibliografía

<https://www.trendmicro.com>

[https://firmar.gob.ar](https://firmar.gob.ar/index.html)

<https://networkradius.com/blog/security/wifi-security-with-radius/>

<https://tools.ietf.org/html/rfc6071>  
  
Manual de procedimientos Política única de certificación de la AC ONTI.